近世代数应用基础

JinShi DaiShu YingYong JiChu

张劼　莫骄◎编著



北京邮电大学出版社
www.buptpress.com

JinShi DaiShu YingYong JiChu

策 划 人：赵玉山

责任编辑：何芯逸

封面设计：


ISBN 978-7-5635-2863-9

9 787563 528639

定价：15.00元

近世代数应用基础

张 劼 莫 骄 编著



北京邮电大学出版社
www.buptpress.com

前　　言

近世代数是一门非常抽象的数学学科. 本书在内容编写上，力争做到抽象概念与具体实例相结合. 对于群、环、域以及扩域这些基本的代数系统，我们都介绍了它们在信息工程中的具体应用. 在内容顺序安排上，力争难点分散. 此外，本教材还具有以下特点：

（1）问题引入. 教材以大家熟悉的问题为切入点，提高大家学习这门课的兴趣。

（2）精炼预备知识. 尽快让学生感受近世代数课程的特点，转换思维模式.

（3）强调域上多项式，淡化一般环上多项式. 降低难度，增强了实用性.

作　者

目　　录

第1章　引言和预备知识

代数学是数学的一个古老分支，有着悠久的历史. 到19世纪时，代数学的研究对象和研究方法发生了巨大的变化. 人们开始关注带有运算的集合，研究方法也从以往偏重计算的思维向结构研究的思维转变，形成了所谓的近世代数学.

具有一种或几种代数运算的集合，称为代数系统. 近世代数(也称抽象代数)是研究各种抽象的代数系统的学科. 根据代数系统中的运算个数及运算所满足的性质的不同，就产生了不同的代数系统，进而形成了近世代数中各个不同的分支，其中最重要、最基本的分支是群、环和域. 目前，关于群、环、域的研究内容和方法不仅渗透到数学的各个学科，而且已经广泛应用到信息科学、计算机科学、物理、化学等诸多学科.

本课程主要介绍近世代数中最基本的代数系统——群、环和域的最基本的概念与性质.

1.1　与近世代数相关的几个问题

1.1.1　数字通信中的可靠问题

现代通信中用数字代表信息，用电子设备进行发送、传递和接收，并用计算机加以处理. 通信系统传输消息必须可靠与快速，但在数字通信系统中可靠与快速往往是一对矛盾. 若要求快速，则必然使得每个数据码元所占的时间缩短，波形变窄，能量减少，从而在受到干扰后产生错误的可能性增加，传送信息的可靠性降低. 若要求可靠，则使得传送消息的速率变慢. 如何较合理地解决可靠性与速度这一对矛盾，是正确设计一个通信系统的关键问题之一. 简单来说编码学就是在解决这对矛盾中不断发展起来的.

编码分为信源编码和信道编码. 信源编码的研究目的是提高传输效率，而信道编码

的研究目的就是提高信号传输的可靠性，纠错码是信道编码的重要研究内容. 下面用两个简单例子来说明纠错码的概念.

重复码是一个简单的纠错码，它的编码规则是一个信息元，剩下的校验元为信息元的重复. 例如，用 3 位二进制重复码表示 A，B 两个字母，A 编码为 000，B 编码为 111，则接收方收到下列信息时均译码为

接收信息：000，001，010，011，101，110，111

译码：　A，　A，　A，B，　B，　B，　B

这就意味着在译码时对其中的错误信息进行了纠正. 其中纠错的理论依据基于在信道中错 1 个比特的概率要高于 2 个比特的假设，并且译码使用了大数准则.

近世代数是进行编码设计的重要工具，较复杂的编码将在后面进行介绍.

1.1.2　数字通信中的保密问题

随着计算机科学的蓬勃发展，社会已进入信息时代. 但是电子计算机和通信网络的广泛应用，一方面为人们的生活和工作提供了便利，另一方面也提出了许多亟待解决的问题，其中信息的安全性就是一个突出的问题. 信息安全的核心技术是密码学，因此，密码学理论和技术已成为信息科学和技术中的一个重要研究领域.

密码技术主要功能是隐藏和保护需要保密的信息，使未授权者不能提取信息. 信息的原文通常称为明文，加密后的信息称为密文. 以下将借助一个古典密码来了解密码的加密解密算法.

美国电话电报公司的 Gilbert Vernam 在 1917 年为电报通信设计了一种非常方便的密码，称为 Vernam 密码. Vernam 密码在对明文加密前首先将明文编码为含有 0，1 的字符串.

设 $m=m_1m_2\cdots m_s\cdots$ 为明文，$k=k_1k_2\cdots k_s\cdots$ 为密钥，其中 m_i,k_i 取值 0 或 1($i\geqslant 1$). 则密文 $c=c_1c_2\cdots c_s\cdots$，其中

$$c_i=m_i\oplus k_i,\quad i\geqslant 1$$

这里$\oplus$为模 2 加法.

在用 Vernam 密码对明文加密时，如果对不同的明文使用不同的密钥，则这时 Vernam 密码为“一次一密”密码，而“一次一密”密码是目前被理论上证明是安全的唯一密码算法. 这种密码的安全性完全取决于密钥的随机性. 但是随机密钥的生成难以实现，并且可以看出使用这种密码无论从时间还是空间上代价都非常大. 如果不同的明文使用相同的密钥，则 Vernam 密码就比较容易破译了.

当“敌手”获取了一个密文 $c=c_1c_2\cdots c_s\cdots$ 所对应的明文 $m=m_1m_2\cdots m_s\cdots$ 时，很容易通过运算 $k_i=m_i\oplus c_i(i\geqslant 1)$ 获得密钥 $k=k_1k_2\cdots k_s\cdots$. 因此如果密钥 k 重复利用，“敌手”可以立即解密得到相应的明文.

当然，现在密码学所使用的密码算法比较复杂，算法中所涉及的运算大多数是基于代数系统的，其中基于域上的运算更多些. 因此近世代数是现代密码学最重要的数学基础. 在后续的内容上将具体介绍.

1.1.3　几何作图问题

古代数学家曾提出过几个有意思的尺(直尺)规(圆规)作图问题，规定所用的直尺没有刻度，也不能在上面作标记.

(1) 立方倍积问题：做一个立方体使其体积为一个已知立方体体积的两倍.

(2) 三等分角问题：给定任意一个角，将其三等分.

(3) 化圆为方问题：给定一个圆，做一个正方形使其面积等于已知圆的面积.

(4) 等分圆周问题：将一个圆等分成 n 份.

以上这些问题描述很简单，但直到近世代数理论出现以后才得到完全解决.

1.1.4　代数方程求根问题

方程及方程组求解是代数学研究的基本问题之一. 对于多元一次方程组的问题，我国睿智的古代数学家们早已给出了解决的办法，《九章算术》中就有专门的一章“方程”来求解此类问题. 运算采用的是被称为“遍乘直除”的方法，而这种方法实际上便是现在常用的解多元一次方程组的加减消元法.

对于一元二次方程的求根公式分别在公元 3 世纪由中国的赵爽及 600 年后的花拉子米提出. 而三次及四次方程的求根公式难住了数学家一千年，直到塔塔利亚和卡丹的出现，才发现了一般的三次和四次方程的求根公式. 18 世纪后，人们开始研究高于四次方程的代数求根的方法，但是屡战屡败. 法国数学家拉格朗日发表论文《关于代数方程解的思考》，他认为次数不低于五次的方程的代数解法一般而言是找不到的，他试图证明这个理论的正确性，但是均以失败告终. 到 19 世纪初，挪威和法国的两位天才的年轻数学家阿贝尔(Abel)和伽罗华(Galois)证明了拉格朗日的猜想，而在他们的研究工作中诞生的新概念和新理论将代数带入了一个新的时代，即抽象代数时代.

1.2 集合和映射

这一节所介绍的集合和映射的概念，在高等代数中已经学习过. 但为了和后面内容更好的衔接，在此重复一下，并统一某些标识符号.

1.2.1 集合

集合其实到目前为止，并没有统一的定义. 一般将若干个(有限或无限)固定事物的全体就叫做一个集合(简称集). 组成一个集合的事物就叫做集合的元素(简称元).

习惯用大写的英文字母表示集合，如 A,B,C 等. 元素用小写英文字母表示，比如 a，b，c 等.

若 a 是集合 A 中的元素，就说 a 属于集合 A，记为 $a\in A$. 否则就说 a 不属于集合 A，记为 $a\notin A$.

没有任何元素的集合称为空集，一般记为 $\varnothing$.

定义 1.2.1 如果集合 B 中的元素都属于集合 A，则称集合 B 是集合 A 的子集. 记为 $B\subseteq A$，或 $A\supseteq B$，读作 A 包含 B，或 B 包含于 A.

规定空集是任何集合的子集.

定义 1.2.2 如果集合 B 是集合 A 的子集，并且在集合 A 中至少存在一个元素不属于 B，则称 B 是集合 A 的真子集. 记为 $B\subset A$，或 $A\supset B$.

定义 1.2.3 如果集合 A 和集合 B 互为子集，则称两个集合相等.

定义 1.2.4 集合 A 和集合 B 的所有公共元素组成的集合，称为 A 和 B 的交集. 记为 $A\cap B$.

定义 1.2.5 由至少属于集合 A 和集合 B 之一的所有元素组成的集合称为 A 和 B 的并集. 记为 $A\cup B$.

定义 1.2.6 集合 A 和集合 B 的笛卡儿积或直积，是由 A 和 B 中所有元素构成的有序对组成的集合，记为 $A\times B$.

具体的，
$$A\times B=\{(a,b)\mid a\in A,b\in B\}$$

直积定义中的集合顺序是不能随意调换的. 例如，设 $\mathbf{Z}$ 是全体整数集，$\mathbf{Q}$ 是全体有理数集，则 $\left(2,\frac{1}{3}\right)\in\mathbf{Z}\times\mathbf{Q}$，但 $\left(2,\frac{1}{3}\right)\notin\mathbf{Q}\times\mathbf{Z}$.

上面集合的交集，并集与直积很容易推广到有限个集合上.

例 1.2.1　设 $A=\{1,2,3\}$，$B=\{-1,2\}$，则

$A\cap B=\{2\}$，$A\cup B=\{1,2,3,-1\}$，

$A\times B=\{(1,-1),(1,2),(2,-1),(2,2),(3,-1),(3,2)\}$.

1.2.2　映射

为了比较不同的集合，引入映射的概念.

定义 1.2.7　设 A,B 为两个非空集合，如果存在某个对应法则 f，使得对 A 中每一个元素 $a\in A$，都有 B 中唯一的元素 $b\in B$ 与之对应，则称 f 为集合 A 到集合 B 的一个映射，记为 $f:A\to B$.

其中 b 称为 a 在映射 f 下的象，记为 $f(a)=b$，a 称为 b 在映射 f 下的原象.

b 的所有原象组成的集合称为 b 的原象集.

若 $\forall b\in B$，都有 $a\in A$，使得 $f(a)=b$，则称映射 f 为满射.

若 $\forall a_1,a_2\in A$，当 $a_1\neq a_2$ 时，有 $f(a_1)\neq f(a_2)$，则称映射 f 为单射.

若 f 既是满射，又是单射，则称 f 为一一映射或一一对应.

特别地，设映射 $f:A\to A$，$f(a)=a$，$\forall a\in A$，称 f 为 A 的恒等映射，记为 id_A.

定义 1.2.8　如果 $\forall a\in A$，$f(a)=g(a)$，则映射 $f:A\to B$ 与 $g:A\to B$ 称为相等的.

例 1.2.2　设 $\mathbf{Z}^+$ 是全体正整数的集合，$\mathbf{R}$ 是全体实数的集合，则 $f(n)=\ln n$，$\forall n\in\mathbf{Z}^+$ 是从 $\mathbf{Z}^+$ 到 $\mathbf{R}$ 的映射. f 是单射，但不是满射.

例 1.2.3　设 $\mathbf{R}^2$ 是实平面上的全体点集，$\mathbf{R}$ 是全体实数集，则 $f(a,b)=b-a$，$\forall(a,b)\in\mathbf{R}^2$ 是从 $\mathbf{R}^2$ 到 $\mathbf{R}$ 的映射. f 是满射，但不是单射.

例 1.2.4　一元函数 $f(x)=\arcsin x$ 是从 $[-1,1]$ 到 $\left[-\frac{\pi}{2},\frac{\pi}{2}\right]$ 的一一映射.

定义 1.2.9　设有映射 $f:A\to B$，$g:B\to C$，定义映射 $gf:A\to C$ 如下：

$$(gf)(a)=g[f(a)],\ \forall a\in A$$

称 gf 为 g 与 f 的复合映射或 g 与 f 的乘积.

类似可定义多个映射的乘积.

映射的合成有下面的性质：

性质 1.2.1　映射的复合满足结合律.

即若有 $f:A\to B$，$g:B\to C$，$h:C\to D$，则

$$h(gf)=(hg)f.$$

证明　$\forall a\in A$，记 $f(a)=b,g(b)=c$. 则 $gf(a)=g[f(a)]=g(b)=c$，
且

$$[h(gf)](a)=h[gf(a)]=h(c);$$

又 $hg(b)=h[g(b)]=h(c)$，
所以

$$[(hg)f](a)=(hg)[f(a)]=(hg)(b)=h[g(b)]=h(c).$$

即有 $h(gf)=(hg)f$.

下面的定理给出了一一映射的充要条件.

定理 1.2.1　映射 $f:A\to B$ 为一一映射的充要条件是存在映射 $g:B\to A$，使得 $fg=id_B,gf=id_A$.

证明　充分性. 已知存在映射 $g:B\to A$，使 $fg=id_B,gf=id_A$.

$\forall b\in B$，有 $g(b)\in A$，使 $f[g(b)]=(fg)(b)=b$，故 f 为满射.

$\forall a_1,a_2\in A$，当 $a_1\neq a_2$ 时，若 $f(a_1)=f(a_2)$，则 $g[f(a_1)]=g[f(a_2)]$，由此推出 $(gf)(a_1)=a_1=(gf)(a_2)=a_2$，与 $a_1\neq a_2$ 矛盾，故 $f(a_1)\neq f(a_2)$，f 为满射.

f 既为单射又为满射，所以 f 为一一映射.

必要性. 若 f 是一一映射，下面来构造映射 $g:B\to A$，使 $fg=id_B,gf=id_A$.

$\forall b\in B$，f 是一一映射，故有唯一的 $a\in A$，使得 $f(a)=b$，规定 $g(b)=a$. 这样定义的 g 是从 B 到 A 的映射.

$\forall b\in B,(fg)(b)=f[g(b)]=f(a)=b$，即 $fg=id_B$.

又 $\forall a\in A,(gf)(a)=g[f(a)]=a,gf=id_A$.

若 f 是一一映射，称上述映射 g 为 f 的逆映射，记为 $g=f^{-1}$，由定理 1.2.1 可知 g 也是一一映射.

1.3　代数运算及运算律

定义 1.3.1　一个从集合 $A\times B$ 到集合 D 的映射 $f:A\times B\to D$ 称为一个从 $A\times B$ 到 D 的代数运算.

一般用$\circ$表示这个运算，即 $\forall (a,b)\in A\times B$，将 $f((a,b))$ 记为 $a\circ b$.

若$\circ$是从 $A\times A$ 到 A 的代数运算，即 $\forall a,b\in A,a\circ b\in A$，则称$\circ$是 A 的代数运算或称$\circ$是 A 的二元运算. 当然 A 对于运算$\circ$是封闭的.

例 1.3.1　设 A_1 为所有 2×3 阶实矩阵构成的集合，A_2 为所有 3×2 阶实矩阵构成的集合，A_3 为所有 2 阶实矩阵构成的集合. $\forall A\in A_1$，$\forall B\in A_2$，

$$A\circ B\overset{\text{定义}}{=}AB(\text{矩阵乘积}),$$

则$\circ$为 $A_1\times A_2$ 到 A_3 的代数运算，这个运算就是矩阵的乘法.

例 1.3.2　设 $\mathbf{R}$ 为全体实数集，$A=\{\ln x\mid x>0,x\in\mathbf{R}\}$. $\forall \ln a,\ln b\in A$，定义

$$\ln a\circ\ln b=\ln ab(=\ln a+\ln b),$$

则$\circ$是 A 的代数运算，这个运算就是普通数的加法.

定义 1.3.2　称一个 $A\times A$ 到 A 的代数运算$\circ$满足结合律，如果 $\forall a,b,c\in A$，有

$$(a\circ b)\circ c=a\circ(b\circ c).$$

如果 A 的代数运算$\circ$适合结合律，用数学归纳法可以证明，对 A 的任意 n 个元素 a_1，a_2，…，a_n 来说，所有的 $\pi(a_1\circ a_2\circ\cdots\circ a_n)$都相等，我们用 $a_1\circ a_2\circ\cdots\circ a_n$ 来表示这个唯一的结果. 其中 $\pi(a_1\circ a_2\circ\cdots\circ a_n)$表示对 $a_1\circ a_2\circ\cdots\circ a_n$ 用某种两两加括号的步骤运算后所得到的结果.

例如，$a_1\circ a_2\circ a_3=(a_1\circ a_2)\circ a_3=a_1\circ(a_2\circ a_3)$；

$a_1\circ a_2\circ a_3\circ a_4=(a_1\circ a_2)\circ a_3\circ a_4=a_1\circ(a_2\circ a_3)\circ a_4=a_1\circ a_2\circ(a_3\circ a_4)$.

定义 1.3.3　称一个 $A\times A$ 到 D 的代数运算$\circ$满足交换律，如果 $\forall a,b\in A$，有

$$a\circ b=b\circ a.$$

同样，用数学归纳法可以证明，当 A 的代数运算$\circ$同时适合结合律与交换律时，$a_1\circ a_2\circ\cdots\circ a_n$ 中元素的次序可以调换.

结合律和交换律描述的是一种代数运算的性质. 两种代数运算之间的性质用分配律描述.

设$\odot$是 $B\times A$ 到 A 的代数运算，$\oplus$是 A 的代数运算. $\forall b\in B$，$\forall a_1,a_2\in A$，$b\odot(a_1\oplus a_2)$，$(b\odot a_1)\oplus(b\odot a_2)$都有意义，且都是 A 中的元素，但它们不一定相等.

定义 1.3.4　设$\odot$是 $B\times A$ 到 A 的代数运算，$\oplus$是 A 的代数运算，称代数运算$\odot$，$\oplus$满足右分配律，如果 $\forall b\in B$，$\forall a_1,a_2\in A$，有

$$b\odot(a_1\oplus a_2)=(b\odot a_1)\oplus(b\odot a_2).$$

例如，假设 B 和 A 都是全体实数的集合，$\odot$和$\oplus$是普通的乘法和加法，上式就变成了

$$b(a_1+a_2)=(ba_1)+(ba_2).$$

定义 1.3.5　设$\odot$是 $A\times B$ 到 A 的代数运算，$\oplus$是 A 的代数运算，称代数运算$\odot$，$\oplus$满足左分配律，如果 $\forall b\in B$，$\forall a_1,a_2\in A$，有

$$(a_1\oplus a_2)\odot b=(a_1\odot b)\oplus(a_2\odot b).$$

用数学归纳法可以证得，如果$\oplus$满足结合律，且$\odot$和$\oplus$满足右分配律，那么$\forall b \in B$，$\forall a_1, a_2, \cdots, a_n \in A$，有

$$b \odot (a_1 \oplus a_2 \oplus \cdots \oplus a_n) = (b \odot a_1) \oplus (b \odot a_2) \oplus \cdots \oplus (b \odot a_n).$$

同样，如果$\odot$和$\oplus$满足左分配律，就有

$$(a_1 \oplus a_2 \oplus \cdots \oplus a_n) \odot b = (a_1 \odot b) \oplus (a_2 \odot b) \oplus \cdots \oplus (a_n \odot b).$$

分配律的重要性在于它刻画了两种代数运算的联系，使两种运算融合到一起.

1.4 等价关系与集合的分划

定义 1.4.1 设A是集合，集合$A \times A$的每个子集R称为集合A上的一个(二元)关系. 若$(a,b) \in R$，则称a和b有关系R，写成aRb.

例 1.4.1 设$\mathbf{R}$为全体实数集，$\mathbf{R} \times \mathbf{R}$中的子集$R = \{(a,b) \in \mathbf{R} \times \mathbf{R} \mid a > b\}$就是$\mathbf{R}$上的一个关系，$aRb$指的是$a > b$.

例 1.4.2 设$\mathbf{Z}$为全体整数集，$\mathbf{Z} \times \mathbf{Z}$中的子集$R = \{(a,b) \in \mathbf{Z} \times \mathbf{Z} \mid 3 \text{ 整除} (a-b)\}$就是$\mathbf{Z}$上的一个关系. mRn指的是$m - n = 3k, k \in \mathbf{Z}$，即$m$与$n$模 3 同余，记为$m \equiv n \pmod 3$.

本课程关心的是等价关系，定义如下：

定义 1.4.2 集合A的一个二元关系R称为等价关系，如果它满足以下三条性质：

(1) 反身性：$\forall a \in A, aRa$；

(2) 对称性：$\forall a, b \in A$，若aRb，则bRa；

(3) 传递性：$\forall a, b, c \in A$，若aRb, bRc，则aRc.

若R是等价关系，则aRb记为$a \sim b$. 例 1.4.2 中的二元关系是等价关系，例 1.4.1 中的二元关系就不是等价关系.

定义 1.4.3 若把集合A分成若干个子集，使得A中的每一个元素属于且只属于一个子集，则称这些子集的全体为集合A的一个分划. 每个子集称为A的一个类.

等价关系与集合的分划是一一对应的.

定理 1.4.1 集合A的一个分划决定A的一个等价关系.

证明 给定A的一个分划后，集合A被分成若干个类的并，A中的每一个元素属于且只属于一个类.

令$R = \{(a,b) \in A \times A \mid a \text{ 与 } b \text{ 在同一类}\}$，下面证明$R$是$A$上的一个等价关系.

第一，$\forall a\in A$，因为$(a,a)\in A\times A$，且 a 与 a 在同一类，所以$(a,a)\in R$，即 aRa，这说明 R 具有反身性；第二，$\forall a,b\in A$，如果 aRb，即$(a,b)\in R$，则 a 与 b 在同一类，于是$(b,a)\in R$，即 bRa，这说明 R 具有对称性；第三，$\forall a,b,c\in A$，如果 aRb,bRc，即$(a,b)\in R,(b,c)\in R$，因此 a 与 b 在同一类，b 与 c 在同一类，所以 a 与 c 在同一类，故$(a,c)\in R$，即 aRc，这说明 R 具有传递性.

定理 1.4.2　集合 A 的一个等价关系～决定 A 的一个分划.

证明　记$[a]=\{b\in A\mid b\sim a\}$，即$[a]$是所有与 a 等价的元素全体，称为 a 所在的等价类，a 是代表元.

下面证明 $A=\bigcup_{a\in A}[a]$是 A 的一个分划. 先说明等价类与代表元无关，即若 $a\sim b$，则$[a]=[b]$.

事实上，若 $c\in[a]$，则 $c\sim a$，又 $a\sim b$，由等价关系的传递性可知 $c\sim b$，所以 $c\in[b]$，故$[a]\subseteq[b]$.

类似可证明$[b]\subseteq[a]$，因此$[a]=[b]$.

再来说明 A 中任意元必属于且仅属于某一个类. $\forall a\in A$，易知 $a\in[a]$；若 $a\in[b]$且 $a\in[c]$，则 $b\sim a,a\sim c$，于是 $b\sim c,[b]=[c]$.

定义 1.4.4　设集合 A 有一个分划，每类中的任意元素称为该类的一个代表. 刚好由每一类的一个代表所构成的集合叫做 A 的完全代表系.

如例 1.4.2 中的等价关系确定了 $\mathbf{Z}$ 的一个分划，在这个分划下 $\mathbf{Z}$ 的完全代表系为$\{0,1,2\}$.

其中$[0]=\{3k\mid k\in\mathbf{Z}\}$；$[1]=\{3k+1\mid k\in\mathbf{Z}\}$；$[2]=\{3k+2\mid k\in\mathbf{Z}\}$.

$[0],[1],[2]$称为模 3 的剩余类.

最后介绍本节的另一个重要概念.

定义 1.4.5　设集合 A 中有代数运算$\circ$，若 A 的一个等价关系～满足

$$\forall a,b,c,d\in A, a\sim b, c\sim d\Rightarrow a\circ c\sim b\circ d,$$

则称～为$\circ$的一个同余关系. $a\in A$ 所在的等价类$[a]$称为 a 的同余类.

例 1.4.3　设 m 为正整数，$\mathbf{Z}$ 为全体整数的集合，在 $\mathbf{Z}$ 中定义关系～：

$$a\sim b\Leftrightarrow a\equiv b \pmod m.$$

易证～是等价关系. 且由 $a\equiv b\pmod m$，$c\equiv d\pmod m$，可得

$$a+c\equiv b+d \pmod m,\ ac\equiv bd \pmod m.$$

因此～对于 $\mathbf{Z}$ 中的加法和乘法都是同余关系.

习　题

1. 设 A,B 是两个非空的有限集合.

(1) A 到 B 的不同映射共有多少个?

(2) A 上不同的二元运算共有多少个?

2. 设 A,B 为非空集合,$f:A\to B$ 是集合的映射,试证:

(1) f 为单射$\Leftrightarrow$存在 $g:B\to A$,使得 $gf=id_A$;

(2) f 为满射$\Leftrightarrow$存在 $h:B\to A$,使得 $fh=id_B$.

3. 下面的二元运算$\circ$哪些满足交换律,哪些满足结合律.

(1) 设 $\mathbf{Z}$ 为全体整数的集合,在 Z 中 $a\circ b=a-b$;

(2) 设 $\mathbf{Q}$ 为全体有理数的集合,在 Q 中 $a\circ b=ab+1$;

(3) 设 $\mathbf{Z}^+$ 为全体正整数的集合,在 Z^+ 中 $a\circ b=2^{ab}$;

(4) 在 $\mathbf{Z}^+$ 中 $a\circ b=a^b$.

4. 假设 R 是非空集合 A 中的一个关系,且有对称性和传递性. 有人断定 R 是一个等价关系,其推理如下:"对 $a,b\in A$,从 aRb 得 bRa,又从传递性得 aRa,因而 R 有反身性,故为等价关系."他的推理对吗?

5. 设 R 是非空集合 A 中的任一关系,再定义 A 中关系 R_1,R_2 分别为

xR_1y,当且仅当 $x=y,xRy$ 与 yRx 三者之一成立;

xR_2y,当且仅当有 $x_0,x_1,\cdots,x_n$ 使 $x_0=x,x_n=y$,且 $x_0R_1x_1,x_1R_1x_2,\cdots,x_{n-1}R_1x_n$.

(1) 证明 R_2 是一个等价关系(提示:先证 R_1 具有对称性);

(2) 证明若 R 是等价关系,则 $R_2=R$,即 $xR_2y\Leftrightarrow xRy$;

(3) 令 $A=\mathbf{Z}$ 为全体整数的集合,n 为一固定整数,R 定义为:$xRy\Leftrightarrow x-y=n$,求关系 R_1 与 R_2.

第2章　群

近世代数的主要研究对象是带有运算的集合(称之为代数系统).本课程将介绍三大代数系统:群、环与域.本章先讨论群,着重介绍群的基本概念、基本理论及某些群的结构.

2.1　群的概念

2.1.1　群的定义

定义 2.1.1　设 G 是带有某个二元运算(称之为乘法)的非空集合.如果 G 满足(1)～(4),则称 G 为一个群.

(1) G 对于上述运算封闭(由二元运算的定义可知此条成立,此处仅是强调而已);

(2) 上述运算适合结合律,即 $\forall a,b,c\in G,(ab)c=a(bc)$;

(3) 存在元素 $e\in G$,使得 $\forall a\in G,ae=ea=a$,称 e 为 G 的单位元;

(4) $\forall a\in G$,存在 $b\in G$,使 $ab=ba=e$,称 b 为 a 的逆元.

例 2.1.1　全体整数的集合 $\mathbf{Z}$ 关于普通数的加法运算构成一个群,称为整数群.

例 2.1.2　数域 P 上的全体 n 阶可逆方阵的集合 $\mathrm{GL}(n,P)$ 关于矩阵的乘法构成一个群,称为数域 P 上的一般线性群.

例 2.1.3　设 n 为正整数,记模 n 的剩余类全体为 $Z_n=\{[0],[1],\cdots,[n-1]\}$.在 Z_n 上定义 $\oplus$ 运算:

$$[a]\oplus[b]=[a+b].$$

则 Z_n 关于 $\oplus$ 运算(记为加法)构成群,称为模 n 剩余类群.

证明　我们逐条验证 Z_n 关于 $\oplus$ 满足定义 2.1.1 中的(1)～(4).

(1)先证明 $\oplus$ 是代数运算,即是 $Z_n\times Z_n$ 到 Z_n 的映射.也就是要说明运算与剩余类的

代表元选择无关. 即任取 $a_1\in[a]$, $b_1\in[b]$,有 $[a_1+b_1]=[a+b]$.

事实上,因为 $a_1\in[a]$, $b_1\in[b]$,所以 $n\mid(a_1-a)$, $n\mid(b_1-b)$,故

$$n\mid[(a_1+b_1)-(a+b)],$$

即 $[a_1+b_1]=[a+b]$. 这说明 Z_n 对于运算 $\oplus$ 满足(1).

(2) $\forall[a],[b],[c]\in Z_n$,

$$([a]\oplus[b])\oplus[c]=[(a+b)+c]=[a+(b+c)]=[a]\oplus([b]\oplus[c]).$$

这说明上述运算适合结合律.

(3) 因为 $[a]\oplus[0]=[0]\oplus[a]=[a]$,所以 $[0]$ 为单位元.

(4) 因为 $[a]\oplus[n-a]=[n-a]\oplus[a]=[0]$,所以 $[n-a]$ 是 $[a]$ 的逆元.

综上,Z_n 关于 $\oplus$ 运算(记为加法)构成群.

例 2.1.4 设 $\mathbf{Z}$ 为整数集,在 $\mathbf{Z}$ 上定义运算

$$a\circ b=a+b-3.$$

求证:$\mathbf{Z}$ 关于 $\circ$ 构成群.

证明 首先容易验证 $\circ$ 为 $\mathbf{Z}$ 上的二元运算. $\forall a,b,c\in\mathbf{Z}$,

因为 $a\circ b=a+b-3\in\mathbf{Z}$,即 $\circ$ 满足封闭性.

$$(a\circ b)\circ c=(a+b-3)\circ c=(a+b-3)+c-3=a+(b+c-3)-3=a\circ(b\circ c)$$

即 $\circ$ 满足结合律.

又 $a\circ 3=3\circ a=a+3-3=a$,即 3 是单位元.

最后,$a\circ(6-a)=(6-a)\circ a=3$,即 $6-a$ 是 a 的逆元.

由群的定义可知 $\mathbf{Z}$ 对此运算构成群.

2.1.2 群的简单性质

先讨论群的一些基本性质.

性质 2.1.1 若 G 是群,则 G 中单位元唯一.

证明 设 e_1,e_2 是群 G 的单位元,则 $\forall a\in G$,满足

$$ae_1=e_1a=a.$$

$$ae_2=e_2a=a.$$

所以

$$e_1=e_1e_2=e_2.$$

性质 2.1.2 若 G 是群,则 $\forall a\in G$,a 的逆元唯一,记为 a^{-1}.

证明 设 b,c 均为 a 的逆元,即 $ab=ba=e$,$ac=ca=e$,其中 e 是群 G 的单位元. 则

$$b=be=b(ac)=(ba)c=ec=c.$$

性质 2.1.3　若 G 是群，则 G 中消去律成立. 即

若 $ax=ay$，则 $x=y$；

若 $xa=ya$，则 $x=y$.

由此可知 $ax=b, ya=b$ 在 G 中解唯一.

证明　若 $ax=ay$，则

$$a^{-1}(ax)=a^{-1}(ay),(a^{-1}a)x=(a^{-1}a)y,x=y;$$

类似可证明若 $xa=ya$，则 $x=y$.

2.1.3　群的等价定义

下面介绍几个群的等价定义，以方便大家对群更好的理解和判断.

定义 2.1.2　设 G 是带有某二元运算的非空集合. 如果 G 满足下面(1)～(4)，则称 G 为一个群.

(1) G 对该运算(称之为乘法)封闭；

(2) 该运算适合结合律；

(3) 存在左单位元 $e_左\in G$，使 $\forall a\in G, e_左 a=a$；

(4) $\forall a\in G$，存在 $a_左^{-1}\in G$，使 $a_左^{-1}a=e_左$，称 $a_左^{-1}$ 为 a 的左逆元.

接下来证明定义 2.1.1 与定义 2.1.2 的等价性.

证明　显然若 G 满足定义 2.1.1 中的条件(1)～(4)，则 G 也满足定义 2.1.2 中的条件(1)～(4).

反之，设 G 满足定义 2.1.2 中的条件(1)～(4).

$\forall a\in G$，设 $a_左^{-1}$ 的左逆元为 b，即 $ba_左^{-1}=e_左$，则

$$(ba_左^{-1})a=e_左 a=a=b(a_左^{-1}a)=be_左,$$

$$aa_左^{-1}=(be_左)a_左^{-1}=ba_左^{-1}=e_左,$$

$$ae_左=a(a_左^{-1}a)=(aa_左^{-1})a=e_左 a=a.$$

这说明 $e_左$ 就是 G 的单位元，且 $a_左^{-1}$ 就是 a 的逆元，于是 G 满足定义 2.1.1 中的条件(1)～(4).

定义 2.1.3　设 G 是带有某二元运算的非空集合. 若 G 满足条件(1)～(3)，则称 G 为一个群.

(1) G 对该运算封闭；

(2) 该运算适合结合律；

(3) $\forall a,b\in G$，$ax=b$ 和 $ya=b$ 在 G 中有解.

下面证明定义 2.1.1 与定义 2.1.3 的等价性.

证明 显然若 G 满足定义 2.1.1 中的条件(1)～(4)，则 G 也满足定义 2.1.3 中的条件(1)～(3).

反之，设 G 满足定义 2.1.3 中的条件(1)～(3).

任取 $a\in G$，设 $xa=a$ 的解为 x_1，即 $x_1a=a$，下面证 x_1 是 G 的左单位元.

$\forall b\in G$，设 $ax_2=b$，则

$$x_1b=x_1(ax_2)=(x_1a)x_2=ax_2=b,$$

这说明 x_1 是左单位元.

再任取 $a\in G$，$ya=x_1$ 在 G 中有解，这说明 a 有左逆元. 因此 G 满足定义 2.1.2，从而满足定义 2.1.1.

定义 2.1.4 (有限群的等价定义)设 G 是带有某二元运算(称之为乘法)的非空有限集合. 若 G 满足条件(1)～(3)，则称 G 是一个群.

(1) G 对该乘法封闭；

(2) 该乘法运算适合结合律；

(3) 该乘法 G 中消去律成立，即 $\forall a,x,y\in G$，都有

$$ax=ay \Rightarrow x=y;$$

$$xa=ya \Rightarrow x=y.$$

下面证明定义 2.1.1 与定义 2.1.4 的等价性.

证明 设 G 是带有某二元运算的非空有限集合. 如果 G 满足定义2.1.1中的条件(1)～(4)，易见 G 也满足定义 2.1.4 中的条件.

反之，若 G 满足定义 2.1.4 中的条件，设 $G=\{a_1,a_2,\cdots,a_n\}$(a_i 两两不同，$1\leqslant i\leqslant n$).

任取 $a\in G$，$aG=\{aa_1,aa_2,\cdots,aa_n\}\subseteq G$，且 $aa_i\neq aa_j$ $(i\neq j)$(否则由消去律可知 $a_i=a_j$)，因此 $aG=G$.

于是 $\forall b\in G$，存在 a_k，使 $aa_k=b$，即 $ax=b$ 在 G 中有解，类似可证 $ya=b$ 在 G 中有解，这说明 G 满足定义 2.1.3，从而满足定义 2.1.1.

2.1.4 相关概念

定义 2.1.5 若群 G 的运算适合交换律，即 $\forall a,b\in G$，有 $ab=ba$，则称 G 为交换群或 Abel 群.

定义 2.1.6　若群 G 只有有限个元素，则称 G 为有限群，否则称为无限群. 有限群 G 的元素个数称为群 G 的阶，记为 $|G|$.

下面先引入群中元素的阶的概念.

设 a 为群 G 的元素，e 为 G 中的单位元，n 为正整数.

规定

$$a^0=e,$$

$$a^n=\overbrace{aa\cdots a}^{n\text{个}},$$

$$a^{-n}=(a^{-1})^n.$$

容易验证，对任意整数 l,k，都有

$$a^ka^l=a^{k+l}.$$

$$(a^k)^l=a^{kl}.$$

定义 2.1.7　设 a 为群 G 的元素，e 为 G 中的单位元. 若存在正整数 m，使 $a^m=e$，则称 a 为有限阶元素，且称

$$\min\{m\,|\,m\text{ 为正整数}, a^m=e\}$$

为 a 的阶.

如果不存在这样的正整数，就称 a 为无限阶元素.

由元素阶的定义，任意群的单位元的阶都是 1.

在整数群中，除了单位元 0 之外，其他元都是无限阶元.

例 2.1.5　求 Z_6 中各元素的阶.

解　[0]是 1 阶元. $[3]^2=[0]$，所以[3]是 2 阶元.

$[2]^3=[0]$，$[4]^3=[0]$，所以[2]，[4]是 3 阶元.

$[1]^6=[0]$，$[5]^6=[0]$，所以[1]，[5]是 6 阶元.

关于元素的阶，我们来证明下面两条性质.

性质 2.1.4　a 是无限阶元$\Leftrightarrow \forall m,n\in \mathbf{Z}^+$，当 $m\neq n$ 时，有 $a^m\neq a^n$，其中 $\mathbf{Z}^+$ 为全体正整数构成的集合.

证明　充分性. 若存在　$m_1,n_1\in \mathbf{Z}^+$，$m_1\neq n_1$，$a^{m_1}=a^{n_1}$，无妨设 $m_1>n_1$，则

$$a^{m_1}a^{-n_1}=a^{n_1}\cdot a^{-n_1}=a^{n_1}\cdot (a^{-1})^{n_1}=e,$$

即 $a^{m_1-n_1}=e$，与 a 是无限阶矛盾.

必要性. 若 a 是有限阶元，设 a 的阶为 k，则

$$\forall m\in \mathbf{Z}^+\text{，有 } a^{k+m}=a^m,$$

这与条件矛盾.

性质 2.1.5 a 与 a^{-1}同阶.

证明 若 a 是无限阶的,则由性质 2.1.4 可知,

$$\forall m,n\in \mathbf{Z}^{+},当\ m\neq n,有\ a^{m}\neq a^{n}.$$

所以

$$(a^{m})^{-1}\neq (a^{n})^{-1},$$

即

$$(a^{-1})^{m}\neq (a^{-1})^{n}.$$

再由性质 2.1.4,可知 a^{-1}也是无限阶的.

反之,如果 a^{-1}是无限阶的,同理可证 a 也是无限阶的. 若 a 是有限阶的,则 a^{-1}也是有限阶的.

分别记 a 与 a^{-1}的阶数为 k_1,k_2,由

$$a^{k_1}=e,$$

可得

$$(a^{k_1})^{-1}=(a^{-1})^{k_1}=e.$$

故 $k_2\leqslant k_1$,类似可证 $k_1\leqslant k_2$,故 $k_1=k_2$.

性质 2.1.6 设 a 的阶是 n,则 $a^m=e$ 的充要条件是 $n|m$.

证明 必要性. 如果 $a^m=e$,设

$$m=nl+r,0\leqslant r\leqslant n-1,$$

则有

$$a^{m}=a^{nl+r}=a^{nl}a^{r}=(a^{n})^{l}a^{r}=a^{r}=e.$$

所以得到 $r=0$,即有 $n|m$.

充分性. 若有 $n|m$,设 $m=nl$,则有

$$a^{m}=a^{nl}=(a^{n})^{l}=e^{l}=e.$$

2.1.5 群的同态

为了比较不同的群,引入群的同态与同构.

定义 1.2.8 设 G_1,G_2 为两个群,f 是从 G_1 到 G_2 的映射. 如果 f 满足:

$$\forall x,y\in G_1,f(xy)=f(x)f(y),$$

则称 f 是 G_1 到 G_2 的一个同态映射.

当 f 是单射,称 f 为单同态映射.

当 f 是满射,称 f 为满同态映射. 此时称群 G_1 与 G_2 同态.

当 f 是一一映射，称 f 为同构映射. 此时也称 G_1 与 G_2 同构，记为 $G_1 \cong G_2$.

群 G 到自身的同构映射称为 G 的自同构.

例 2.1.6　设 G 是 Abel 群，定义映射 $f:G\to G$ 为

$$f(g)=g^{-1},\quad \forall g\in G,$$

则 f 是 G 的自同构.

证明　$\forall x,y\in G$,

$$f(xy)=(xy)^{-1}=y^{-1}x^{-1}=x^{-1}y^{-1}=f(x)f(y),$$

故 f 是同态映射. f 显然是一一映射，因此 f 是 G 的自同构.

例 2.1.7　设 $GL(n,R)$ 代表 n 阶可逆实方阵全体，则 $\mathrm{GL}(n,R)$ 关于矩阵乘法构成一个群. 设 $\mathbf{R}^*$ 代表全体非零实数，则 $\mathbf{R}^*$ 关于数的乘法构成一个群.

定义 $f:\mathrm{GL}(n,R)\to\mathbf{R}^*$ 为

$$f(\boldsymbol{A})=\det\boldsymbol{A},\quad \forall \boldsymbol{A}\in\mathrm{GL}(n,R).$$

可以验证 f 是从 $\mathrm{GL}(n,R)$ 到 $\mathbf{R}^*$ 的映射.

$\forall a\in\mathbf{R}^*$，令

$$\boldsymbol{B}=\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

则有 $f(\boldsymbol{B})=\det\boldsymbol{B}=a$，即矩阵 $\boldsymbol{B}$ 是 a 的原象. f 是满射.

并且，$\forall \boldsymbol{A},\boldsymbol{B}\in\mathrm{GL}(n,R)$，有

$$f(\boldsymbol{AB})=\det(\boldsymbol{AB})=\det\boldsymbol{A}\cdot\det\boldsymbol{B}=f(\boldsymbol{A})f(\boldsymbol{B}),$$

故 $\mathrm{GL}(n,R)$ 与 $\mathbf{R}^*$ 同态.

群的同态有如下性质：

性质 2.1.7　若 f 是群 G_1 到群 G_2 的同态，g 是群 G_2 到群 G_3 的同态. 则 gf 是 G_1 到 G_3 的同态；

若 f,g 都是满同态，则 gf 也是满同态；若 f,g 都是同构，则 gf 也是同构.

证明　已知 f 是从 G_1 到 G_2 的映射，g 是从 G_2 到 G_3 的映射. 由定义 1.2.9 可知 gf 是从 G_1 到 G_3 的映射. 若 f,g 都是满射，则 gf 也是满射；若 f,g 都是一一映射，则 f,g 也是一一映射.

又已知

$$\forall a,b\in G_1,\quad f(ab)=f(a)f(b);$$

$$\forall x,y \in G_2,\quad g(xy)=g(x)g(y).$$

所以

$$gf(ab)=g[f(ab)]=g[f(a)f(b)]=[gf(a)][gf(b)].$$

性质 2.1.8 设 f 是群 G_1 到群 G_2 的同态，则 $f(e_1)$ 是 G_2 的单位元，其中 e_1 是 G_1 的单位元. $\forall a \in G_1$，$f(a^{-1})$ 是 $f(a)$ 的逆元.

证明 因为

$$f(e_1)=f(e_1^2)=f(e_1)f(e_1),$$

故

$$f(e_1)^{-1}f(e_1)=e_2=f(e_1).$$

其中 e_2 代表 G_2 的单位元.

又

$$f(a^{-1})f(a)=f(a^{-1}a)=f(e_1)=e_2=f(a)f(a^{-1}).$$

即 $f(a^{-1})$ 是 $f(a)$ 的逆元.

性质 2.1.9 设 f 是群 G_1 到群 G_2 的同态映射，则

$$f(G_1)=\{f(g)\mid g\in G_1\}\subseteq G_2$$

也是群，并且 G_1 与 $f(G_1)$ 同态.

证明 任取 $f(g_1),f(g_2)\in f(G_1)$，其中 $g_1,g_2\in G_1$，

$$f(g_1)f(g_2)=f(g_1g_2)\in f(G_1).$$

这说明 $f(G_1)$ 关于 G_2 中的乘法是封闭的. 因为 G_2 是群，所以这个乘法运算适合结合律. 由性质 2.1.8 可知，$f(e_1)$ 是 $f(G_1)$ 的单位元，其中 e_1 是 G_1 的单位元. $\forall a\in G_1$，$f(a^{-1})$ 是 $f(a)$ 的逆元.

总之，$f(G_1)$ 是群，且 f 是 G_1 到 $f(G_1)$ 的满射，所以 G_1 与 $f(G_1)$ 同态.

性质 2.1.10 群的同构关系是一个等价关系.

证明 设 G 为任意一个群，则 G 的恒等映射 id_G 是 G 的自同构，这说明群的同构关系具有反身性；

设 G_1,G_2 为群，f 是从 G_1 到 G_2 的同构映射，则 f^{-1} 是从 G_2 到 G_1 的一一映射，且 $\forall b_1,b_2\in G_2$，设 $b_1=f(a_1)$，$b_2=f(a_2)$，可得 $a_1=f^{-1}(b_1)$，$a_2=f^{-1}(b_2)$，

$$f^{-1}(b_1b_2)=f^{-1}[f(a_1)f(a_2)]=f^{-1}[f(a_1a_2)]=a_1a_2=f^{-1}(b_1)f^{-1}(b_2),$$

故 f^{-1} 是从 G_2 到 G_1 的同构，这说明群的同构关系具有对称性；

设 G_1,G_2,G_3 为群，f 是从 G_1 到 G_2 的同构映射，g 是从 G_2 到 G_3 的同构映射，由性质 2.1.7 可知，gf 是从 G_1 到 G_3 的同构映射，这说明群的同构关系具有传递性.

2.2　变换群与置换群

变换群和置换群是一种具体的群，它们和所有的群都有着密切关系. 用它们可以表示出任意的群，因此在群论中占有重要地位.

2.2.1　变换群

定义 2.2.1　集合 A 到自身的一个映射，称为 A 上的一个变换.

前面已经定义过映射的复合. 记 A 的全体变换集合为 S，则映射的复合运算是 S 中的一个运算，我们称之为乘法.

任取 $\sigma,\tau\in S$，$\forall a\in A$，有

$$(\sigma\tau)(a)=\sigma\tau(a).$$
$$=\sigma(\tau(a))$$

另外，任取 $\sigma,\tau,\mu\in S$，$\forall a\in A$，有

$$(\sigma(\tau\mu))(a)=\sigma((\tau\mu)(a))=\sigma(\tau(\mu(a))),$$
$$((\sigma\tau)\mu)(a)=(\sigma\tau)(\mu(a))=\sigma(\tau(\mu(a))).$$

故 $\sigma(\tau\mu)=(\sigma\tau)\mu$.

这说明 S 关于这个乘法运算是封闭的，且该运算适合结合律，值得注意的是，这个乘法运算并不适合交换律.

例 2.2.1　设 $A=\{1,2,3\}$，

$$\sigma{:}1\to2,2\to3,3\to1.$$
$$\tau{:}1\to2,2\to3,3\to2.$$

则

$$\sigma\tau{:}1\to3,2\to1,3\to3.$$
$$\tau\sigma{:}1\to3,2\to2,3\to2.$$

因此 $\sigma\tau\neq\tau\sigma$.

设集合 A 的全体变换为 $S=\{\tau_1,\tau_2,\cdots\}$，则 S 对于上面的乘法并不构成群. 这是因为 $\forall\sigma\in S$，σ 有逆的充要条件是 σ 为一一映射(即一一变换).

定义 2.2.2　由 A 的若干个一一变换构成的群(关于上面的乘法即复合运算)称为 A 的变换群.

首先关心的是究竟有没有 A 的变换群. 下面的定理将作出回答.

定理 2.2.1 集合 A 的全体一一变换(关于复合运算)构成一个变换群 S_A，称之为 A 上的全变换群.

证明 设 A 的全体一一变换的集合为 S_A.

任取 $\sigma,\tau\in S_A$，因为 σ,τ 都是 A 到 A 的一一映射，所以 $\sigma\tau$ 也是 A 到 A 的一一映射，这说明 S_A 关于复合运算封闭.

上面已验证该运算适合结合律. id_A(记为 ε)是 S_A 中的单位元.

$\forall\sigma\in S_A$，有 $\sigma^{-1}\in S_A$，使 $\sigma^{-1}\sigma=\sigma\sigma^{-1}=\varepsilon$.

总之 S_A 关于映射的复合运算构成群.

例 2.2.2 设 $\mathbf{R}^2$ 是实平面上所有点的全体(即 xy 平面)，σ 是 $\mathbf{R}^2$ 的一一变换且保持距离，即

$$\forall x,y\in\mathbf{R}^2,\ \|\sigma(x)-\sigma(y)\|=\|x-y\|.$$

其中 $\|x-y\|$ 表示点 x 与 y 间的距离，G 是所有这样的 σ 的全体.

求证：G 关于映射的复合运算构成一个群.

证明 $\forall\sigma,\tau\in G$，因为 $\|\sigma\tau(x)-\sigma\tau(y)\|=\|\tau(x)-\tau(y)\|=\|x-y\|$，所以 $\sigma\tau\in G$. 映射的复合运算适合结合律. 恒等变换 $\varepsilon\in G$，且 $\forall\sigma\in G$，$\varepsilon\sigma=\sigma\varepsilon=\sigma$，即 ε 是 G 的单位元. $\forall\sigma\in G$，σ^{-1}是一一变换，且

$$\|\sigma^{-1}(x)-\sigma^{-1}(y)\|=\|\sigma\sigma^{-1}(x)-\sigma\sigma^{-1}(y)\|=\|x-y\|,$$

故 $\sigma^{-1}\in G$. 因此 G 关于映射的复合运算构成群.

这个群称之为欧氏运动群(非交换群).

定义 2.2.3 设 G 是群，任取 $a\in G$，定义 G 的两个变换 L_a,R_a 如下：

$$L_a(x)=ax,R_a(x)=xa,\ \forall x\in G.$$

分别称 L_a,R_a 为由 a 决定的左平移与右平移.

很明显，L_a,R_a 都是 G 的一一变换，即为 S_G 中元素，且容易验证下面的等式：

$$L_aL_b=L_{ab},\quad R_aR_b=R_{ba},\quad L_aR_b=R_bL_a,$$

$$L_e=R_e=id_G,\quad L_{a^{-1}}=L_a^{-1},\quad R_{a^{-1}}=R_a^{-1}.$$

其中 e 为 G 的单位元，a,b 为 G 的任意元素.

从上述等式可知 $L_G=\{L_a|a\in G\}$ 与 $R_G=\{R_a|a\in G\}$ 都是变换群.

定理 2.2.2 (Cayley 定理)设 G 是一个群，则 $G\cong L_G\cong R_G$. 即任何一个群都与一个变换群同构.

证明 定义映射 $f:G\to L_G$ 为

$$f(a)=L_a, \quad \forall a\in G.$$

显然 f 是满射.

若 $f(a)=f(b)$,则 $L_a=L_b$,即

$$L_a(e)=ae=a=L_b(e)=be=b,$$

故 f 为单射. 因此 f 是一一映射.

又

$$f(ab)=L_{ab}=L_aL_b=f(a)f(b),$$

因此 f 是同构映射,从而 $G\cong L_G$.

再定义映射 $g:G\to R_G$ 为

$$g(a)=R_{a^{-1}}, \quad \forall a\in G.$$

类似可以证明 $G\cong R_G$.

2.2.2　置换群

置换群是一类特殊的变换群,群论最早就是从研究置换群开始的. 利用这种群,伽罗华成功地解决了代数方程是否可用根式求解的问题.

另外,置换群也是一类重要的非交换群.

定义 2.2.4　一个有限集合 A 的一个一一变换叫做 A 的一个置换.

此时 A 的变换群称为置换群(即由 A 的若干个置换构成的群).

定义 2.2.5　一个包含 n 个元素的集合的全体置换构成的群称为 n 次对称群,记为 S_n.

易见 S_n 的阶为 $n!$.

设 $A=\{a_1,a_2,\cdots,a_n\}$是含有 n 个元素的有限集合,σ 是 A 的一个置换. 设 $\sigma:a_i\to a_{k_i}$,$1\leqslant i\leqslant n$,则将 σ 表为

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_{k_1} & a_{k_2} & \cdots & a_{k_n} \end{pmatrix} \text{或} \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \sigma(a_1) & \sigma(a_2) & \cdots & \sigma(a_n) \end{pmatrix},$$

也可简单的表示为$\begin{pmatrix} 1 & 2 & \cdots & n \\ k_1 & k_2 & \cdots & k_n \end{pmatrix}$.

例如,S_3 中的元 $\sigma:1\to 2,2\to 3,3\to 1$ 可表为

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}=\begin{pmatrix} 2 & 3 & 1 \\ 3 & 1 & 2 \end{pmatrix}=\begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix}.$$

定义 2.2.6 一个置换若把 t 个不同元素 $a_{i_1},a_{i_2},\cdots,a_{i_t}$ 分别映成 $a_{i_2},a_{i_3},\cdots,a_{i_t},a_{i_1}$，而其余的元素(假设有的话)不变，则称这个置换为一个 t－循环置换，或长为 t 的轮换. 表示为

$$(i_1i_2\cdots i_t)\text{或}(i_2i_3\cdots i_ti_1),\cdots,(i_ti_1i_2\cdots i_{t-1}).$$

例如，S_3 中元 $\sigma:1\to2,2\to3,3\to1$ 可表为 $(123)=(231)=(312)$.

定理 2.2.3 任何 n 元置换 π 都可以写成若干个互相没有公共元素的轮换的乘积.

证明 用数学归纳法.

显然当 π 为恒等变换或只变动两个元时定理是对的.

设 π 变动的元素个数 $\leqslant r$ 时定理是对的.

当 π 变动的元素个数为 $r+1$ 时，取一个被 π 变动的元 i_1，设 i_1 变成 i_2，i_2 变成 i_3，这样找下去，直到第一次找到一个 i_k 为止，i_k 被变成 $\{i_1,i_2,\cdots,i_{k-1}\}$ 中的某一个，而不是变成新的元素. i_k 只能被变成 i_1，因为 $i_2,i_3,\cdots,i_{k-1}$ 已经是某个元素的象了，不能再成为 i_k 的象，这样得到一个 k 个元的循环置换 $(i_1i_2\cdots i_k)$. 若 $k=r+1$，则其余元不动，定理得证.

若 $k<r+1$，则其余被变动的元素个数 $\leqslant r$，$\pi=(i_1i_2\cdots i_k)\pi_1$，由假设，$\pi_1$ 可以写成若干个互相没有公共元素的轮换的乘积，从而 π 可以写成若干个互相没有公共元素的轮换的乘积.

定理 2.2.3 告诉我们，任何 n 元置换 π 都可以写成若干个互相没有公共元素的轮换的乘积. 进一步，每个轮换可表成一些对换之积：

$$(a_1a_2\cdots a_n)=(a_1a_n)(a_1a_{n-1})\cdots(a_1a_2),$$

因此每个置换总可以表示为有限个对换之积，这种表达式(甚至对换的个数)显然不唯一，但是同一个置换以多种方式表成对换之积时，其所含对换个数的奇偶性是不变的，能表成奇(偶)数个对换之积的置换称为奇(偶)置换.

全体偶置换记为 A_n，A_n 按复合运算作成群，称之为 n 元交错群.

由 Cayley 定理得到关于置换群的结论.

定理 2.2.4 任何一个有限群都与一个置换群同构.

这个定理说明置换群有资格作为一切有限群的样板群. 但一般情况下，当集合 G 太大，即 $n=|G|$ 太大时，S_n 的子群也不便研究. 为此，抽象代数中经常采取一种方法，即通过讨论群在较小集合 Σ 上的置换表示来研究 G.（因为 $n=|\Sigma|$ 越小，S_n 的子群越容易搞清楚）

2.3　子群与陪集分解

子群是群论的一个基本概念. 研究群的重要方法之一，就是利用子群的性质来推测群的性质，特别地，有时要根据子群的各种特征来对群进行分类.

2.3.1　子群的概念

定义 2.3.1　设 H 为群 G 的非空子集，如果 H 对于 G 的乘法构成群，则称 H 为 G 的子群.

例 2.3.1　$\{e\}$，G 都是群 G 的子群，称为 G 的平凡子群. 除了 $\{e\}$ 和 G 以外，G 的其他子群(如果还有的话)都称为 G 的非平凡子群.

例 2.3.2　整数集 $\mathbf{Z}$ 是有理数集 $\mathbf{Q}$ 的(加法)子群，$\mathbf{Q}$ 是实数集 $\mathbf{R}$ 的(加法)子群. 正交矩阵全体 $O_n(R)$ 是 $GL(n,R)$ 的(乘法)子群.

定理 2.3.1　群 G 的非空子集 H 是 G 的子群的充要条件是 $\forall a,b\in H, ab\in H$，且 $a^{-1}\in H$.

证明　必要性. H 是群，故 $\forall a,b\in H, ab\in H$.

考虑映射 $f: H\to G$，

$$\forall h\in H, f(h)=h,$$

则 f 为同态映射.

设 e_H 为 H 的单位元，由性质 2.1.8 可知，$f(e_H)$ 是 G 的单位元；

$\forall a\in H$，设 a_H^{-1} 是 a 在 H 中的逆元，由性质 2.1.8 可知，$f(a_H^{-1})$ 是 $f(a)$ 在 G 中的逆元；

又 G 中单位元 e_G 与 $a\in H\subset G$ 的逆元都唯一，因此 $f(e_H)=e_G$，$f(a_H^{-1})=a_G^{-1}=a_H^{-1}$，故 $a^{-1}\in H$.

充分性. 此时 H 对乘法封闭，且 a 有逆 a^{-1}，所以 $aa^{-1}=e_G\in H$，H 中有单位元，所以 H 构成群.

推论 2.3.1　若 H 是 G 的子群，则 H 中的单位元就是 G 中的单位元，$\forall a\in H$，a 在 H 中的逆元就是 a 在 G 中的逆元.

定理 2.3.2　群 G 的非空子集 H 是 G 的子群的充要条件是 $\forall a,b\in H, ab^{-1}\in H$.

证明　必要性. H 是子群，由定理 2.3.1 可知，$\forall a,b\in H$，$b^{-1}\in H$，所以 $ab^{-1}\in H$.

充分性. $\forall a\in H, aa^{-1}=e\in H$，且 $ea^{-1}=a^{-1}\in H$，因此 $\forall a,b\in H, b^{-1}\in H$，$a(b^{-1})^{-1}=ab\in H$，$H$ 是群.

定理 2.3.3 群 G 的非空有限子集 H 是 G 的子群的充要条件是 $\forall a,b\in H, ab\in H$.

证明 必要性. 由定理 2.3.2 可知，$\forall a,b\in H, eb^{-1}=b^{-1}\in H$，所以 $a(b^{-1})^{-1}=ab\in H$.

充分性. 因 H 为有限子集，根据定义 2.1.4，只需证明 H 中消去律成立.

$\forall a,h_1,h_2\in H, a,h_1,h_2\in G$，因 G 中有消去律，故

$$ah_1=ah_2\Leftrightarrow h_1=h_2, h_1a=h_2a\Leftrightarrow h_1=h_2,$$

因此 H 中消去律成立，H 构成(有限)群.

例 2.3.3 $C(G)=\{g\in G\mid \forall a\in G, ag=ga\}$称为群 G 的中心. 验证 $C(G)$是群 G 的子群.

证明 因为 G 的单位元在 $C(G)$中，所以 $C(G)$非空.

任取 $g_1,g_2\in C(G)$，则 $\forall a\in G$，有

$$(g_1g_2)a=g_1(g_2a)=g_1(ag_2)=a(g_1g_2),$$

即 $g_1g_2\in C(G)$.

又

$$g_1a=ag_1\Leftrightarrow g_1^{-1}a=ag_1^{-1},$$

即 $g_1^{-1}\in C(G)$. 由定理 2.3.1，$C(G)$是 G 的子群.

2.3.2 子群的陪集分解

下面利用子群对群进行分类，然后推出群的一些重要结论.

定义 2.3.2 设 H 是群 G 的子群，$\forall a\in G$，称集合

$$aH=\{ah\mid h\in H\}$$

为 H 的一个左陪集.

称

$$Ha=\{ha\mid h\in H\}$$

为 H 的一个右陪集.

例 2.3.4 设 $G=S_3, H=\{\varepsilon,(12)\}$($\varepsilon$ 是恒等映射)是 G 的子群，H 的左陪集有以下三个：

$$\varepsilon H=H=(12)H=\{(12),\varepsilon\},$$

$$(13)H=(123)H=\{(123),(13)\},$$

$$(23)H=(132)H=\{(23),(132)\}.$$

H 的右陪集也有三个：

$$H\varepsilon=H=H(12)=\{\varepsilon,(12)\},$$

$$H(13)=H(132)=\{(13),(132)\},$$

$$H(23)=H(123)=\{(123),(23)\}.$$

可见左陪集与右陪集不同，$H(13)\neq(13)H$.

H 的全体左陪集或右陪集正好是群 G 的一个分划，下面加以证明.

性质 2.3.1　$\forall a,b\in G, aH=bH$ 或 $aH\cap bH=\varnothing$（$\varnothing$ 代表空集）.

证明　若 $aH\cap bH\neq\varnothing$，设 $ah_1=bh_2\in aH\cap bH$，下面证明 $aH=bH$.

$\forall h\in H$，有

$$ah=(bh_2h_1^{-1})h=b(h_2h_1^{-1}h)\in bH$$

故 $aH\subseteq bH$，同理 $bH\subseteq aH$，故 $aH=bH$.

由性质 2.3.1 可知，

$$G=\bigcup_{a\in G}aH$$

是 G 的一个分划，类似

$$G=\bigcup_{a\in G}Ha$$

也是 G 的一个分划.

性质 2.3.2　设

$$R=\{(a,b)\mid a\in G,b\in G,aH=bH\},$$

则 R 是 G 中的一个等价关系（将该等价关系记为～），并且

$$\forall a,b\in G,\quad a\sim b\Leftrightarrow a^{-1}b\in H.$$

证明　先证明 $R=\{(a,b)\mid a,b\in G,aH=bH\}$ 是 G 中的一个等价关系.

因为 $aH=aH$，故 $a\sim a$（反身性）；

若 $aH=bH$，则 $bH=aH$，即若 $a\sim b$，则 $b\sim a$（对称性）；

若 $aH=bH, bH=cH$，则 $aH=cH$，即若 $a\sim b, b\sim c$，则 $a\sim c$（传递性）.

再证 $\forall a,b\in G, a\sim b$（即 $aH=bH$）的充要条件是 $a^{-1}b\in H$.

必要性. $aH=bH$，设 $ah_1=bh_2$，于是 $a^{-1}b=h_1h_2^{-1}\in H$.

充分性. 设 $a^{-1}b=h_0\in H$，$\forall h\in H$，有

$$ah=bh_0^{-1}h\in bH,$$

$$bh=ah_0h\in aH.$$

故 $aH=bH$，即 $a\sim b$.

类似有下面的性质.

性质 2.3.3 设 $R_1=\{(a,b)|a\in G,b\in G,Ha=Hb\}$,则 R_1 是 G 中的一个等价关系(将这个等价关系记为～),并且 $\forall a,b\in G,a\sim b$ 的充要条件是 $ab^{-1}\in H$.

性质 2.3.3 的证明与性质 2.3.2 的证明是完全类似的,在此不另赘述.

接下来,讨论子群 H 的左陪集,右陪集的个数.

定理 2.3.4 一个子群 H 的右陪集个数和左陪集个数相同,它们或者都是无限大,或者都是有限并相等.

证明 设 H 的左陪集全体为 $S_左$,右陪集全体为 $S_右$. 定义 $f:S_左\to S_右$ 为

$$\forall aH\in S_左,\quad f(aH)=Ha^{-1}.$$

先证明 f 是从 $S_左$ 到 $S_右$ 的映射.

事实上,根据性质 2.3.2,若 $aH=bH$,则 $a^{-1}b\in H,b^{-1}a\in H$,从而

$$b^{-1}(a^{-1})^{-1}\in H.$$

由性质 2.3.3 可知,$Hb^{-1}=Ha^{-1}$,即 $f(aH)=f(bH)$,这说明 f 是映射.

显然 f 是满射.

又若 $f(aH)=f(bH)$,即 $Hb^{-1}=Ha^{-1}$,则

$$a^{-1}(b^{-1})^{-1}=a^{-1}b\in H,$$

故 $aH=bH$,故 f 为单射.

综上,f 为一一映射,故 $S_左$ 与 $S_右$ 的元素个数或者都为无限大,或者都有限并相等.

定义 2.3.3 群 G 的子群 H 的右陪集(或左陪集)个数,称为 H 在 G 里的指数,记为 $[G:H]$.

关于指数,有下面的定理.

定理 2.3.5 (Lagrange 定理)设 G 为有限群,H 是 G 的子群,则

$$|G|=|H|[G:H].$$

证明 设 $G=\bigcup\limits_{a\in G}aH$ 为 G 的一个分划.

设 $H=\{h_1,h_2,\cdots,h_k\}$,则 $aH=\{ah_1,ah_2,\cdots,ah_k\}$.

又 $ah_i=ah_j$ 的充要条件是 $h_i=h_j$,$1\leqslant i,j\leqslant k$($H$ 中有消去律). 因此 H 与 aH 所含的元素个数相同,即每个左陪集中所含元素个数相同,因此有 $|G|=|H|[G:H]$.

推论 2.3.2 设 H 是有限群 G 的子群,则 $|H|$ 整除 $|G|$.

推论 2.3.3 设 a 是有限群 G 的任意元,则 a 的阶整除 $|G|$.

证明 设 a 的阶为 m,则 $H=\{e,a,a^2,\cdots,a^{m-1}\}$ 是群 G 的子群,且 $|H|=m$. 由推论 2.3.2 即得.

2.4 循环群

对群的研究一般包括群中元素的表达方式，运算规则，在同构意义下的群的分类以及它的子群结构. 这些问题完全分析清楚的群并不多，而循环群是其中一类.

2.4.1 群的生成

定义 2.4.1 设 G 为群，S 是 G 的子集，G 中包含 S 的最小子群 A 叫做由 S 生成的子群，记为 $A=\langle S\rangle$，S 称为 A 的生成组，或称为 A 的生成元系.

若 $G=\langle S\rangle$，S 是有限群，则称 G 为有限生成群.

例如，设 Z 是整数加群，令 $M=\{-2,2\}$，则 $\langle M\rangle$ 是偶数加群. 而且 $\{2,4\}$，$\{4,6,8\}$，$\{-10,4,8\}$ 等是 $\langle M\rangle$ 的生成组.

定理 2.4.1 设 S 是群 G 的非空子集，$S^{-1}=\{a^{-1}\mid a\in S\}$，则

$$\langle S\rangle=\{x_1x_2\cdots x_m\mid x_i\in S\cup S^{-1},1\leqslant i\leqslant m,m\in Z^+\}.$$

证明 令

$$\overline{S}=\{x_1x_2\cdots x_m\mid x_i\in S\cup S^{-1},1\leqslant i\leqslant m,m\in Z^+\},$$

只需证明两点：第一，$\overline{S}$ 是子群且 $S\subseteq\overline{S}$；第二，对任意包含 S 的子群 A，$\overline{S}\subseteq A$.

先证第一点：明显有 $S\subseteq\overline{S}$. 下面证 $\overline{S}$ 是子群.

任取 $a,b\in\overline{S}$，设 $a=x_1x_2\cdots x_m$，$b=y_1y_2\cdots y_n$，其中 $m,n\in Z^+$，$x_1,x_2,\cdots x_m,y_1,y_2,\cdots,y_n\in S\cup S^{-1}$. 则

$$ab^{-1}=(x_1x_2\cdots x_m)(y_1y_2\cdots y_n)^{-1}=x_1x_2\cdots x_my_n^{-1}\cdots y_1^{-1}\in\overline{S},$$

故 $\overline{S}$ 为子群.

再证第二点：对任意包含 S 的子群 A，因为 $S\subseteq A$，故 $S^{-1}\subseteq A$，因此 $\overline{S}\subseteq A$.

2.4.2 循环群定义

定义 2.4.2 由一个元素生成的群 $G=\langle a\rangle$ 称为循环群，a 称为 G 的一个生成元.

由定理 2.4.1 可知 $G=\langle a\rangle=\{a^k\mid k\in Z\}$.

例 2.4.1 Z 对于普通加法构成的整数加群是循环群，且有 $Z=\langle 1\rangle$.

例 2.4.2 设 n 为正整数，模 n 的剩余类加群 Z_n 也是循环群，且有 $Z_n=\langle[1]\rangle$.

关于循环群的结构，有如下的定理：

定理 2.4.2 若 G 是循环群，a 为 G 的生成元，则当 a 为无限阶元时，G 与整数加群同构，a 的阶为有限正整数 n 时，G 与模 n 的剩余类加群 Z_n 同构.

证明 当 a 为无限阶元时，由性质 2.1.4 可知，

$$a^m=a^n \Leftrightarrow m=n, \quad \forall m,n\in Z^+;$$

再由 2.1 节性质 2.1.5 有

$$a^{\ k}=a^{\ l} \Leftrightarrow k=l, \quad \forall k,l\in Z^+.$$

总之，

$$a^m=a^n \Leftrightarrow m=n, \quad \forall m,n\in Z.$$

定义映射 $f:G\to Z$ 为

$$f(a^k)=k, \quad \forall k\in Z.$$

易见 f 是从 G 到 Z 的映射，显然是满射；

若 $f(a^m)=f(a^n)$，则 $m=k$，当然 $a^m=a^k$，因此 f 是单射. 故 f 是一一映射.

又

$$f(a^{k_1}\cdot a^{k_2})=f(a^{k_1+k_2})=k_1+k_2=f(a^{k_1})+f(a^{k_2}),$$

故 f 为同构映射，即 $G\cong Z$.

当 a 的阶为有限正整数 n 时，定义 $f:G\to Z_n$ 为 $f(a^k)=[k]$，$0\leqslant k\leqslant n-1$.

易见 f 是从 G 到 Z_n 的映射，且为满射；

若 $f(a^m)=f(a^k)$，即 $[m]=[k]$，$0\leqslant m,k\leqslant n-1$，则 $m=k$，当然 $a^m=a^k$，因此 f 是单射，故 f 是一一映射. 又

$$f(a^{k_1}\cdot a^{k_2})=f(a^{k_1+k_2})=[k_1+k_2]=[k_1]+[k_2]=f(a^{k_1})+f(a^{k_2}),$$

故 f 为同构映射，即 $G\cong Z_n$.

该定理告诉我们，同阶的循环群同构，所以循环群本质上只有一个.

具体地，设 $G=\langle a\rangle$.

如果 a 是无限阶元，G 的元是

$$\cdots,a^{-2},a^{-1},a^0=e,a,a^2,\cdots.$$

G 中的运算法则是

$$a^h a^k=a^{h+k}.$$

如果 a 的阶是 n，G 的元是

$$a^0=e,a,a^2,\cdots,a^{n-1}.$$

G 中的运算法则是

$$a^h a^k = a^r.$$

这里 $h+k=mn+r, 0 \leqslant r \leqslant n-1$.

因此循环群的存在问题，数量问题，构造问题都已解决了.

2.4.3　循环群的生成元与子群

先看看元素的阶的性质.

定理 2.4.3　设 g,h 为群 G 的元素，则有下面的结论：

(1) 若 g 是 n 阶元素，则对每个正整数 m，g^m 的阶是 $\frac{n}{(m,n)}$；

(2) 若 $gh=hg$，g,h 的阶分别为 n,m，且 $(m,n)=1$，则 gh 的阶是 nm.

证明　(1) 设 g^m 的阶是 k，则 $(g^m)^k = g^{mk} = e$，由性质 2.1.6 可得：

$$n \mid mk,$$

从而

$$\frac{n}{(m,n)} \,\Big|\, \frac{m}{(m,n)} \cdot k,$$

而

$$\left(\frac{n}{(m,n)}, \frac{m}{(m,n)}\right) = 1,$$

因此

$$\frac{n}{(m,n)} \,\Big|\, k.$$

又

$$(g^m)^{\frac{n}{(m,n)}} = g^{\frac{mn}{(m,n)}} = (g^n)^{\frac{m}{(m,n)}} = e,$$

故

$$k \,\Big|\, \frac{n}{(m,n)}.$$

所以

$$k = \frac{n}{(m,n)}.$$

(2) 设 gh 的阶为 k，则有

$$(gh)^{mn} = g^{mn} h^{mn} = e,$$

故 $k \mid mn$.

考虑群 $S = \langle g \rangle \cap \langle h \rangle$，设 S 的阶为 r. 因为 $S \subseteq \langle h \rangle$，由 Lagrange 定理(定理2.3.5)可

得 $r|m$.

又因为 $S\subseteq\langle g\rangle$，同理可知 $r|n$，故 $r|(m,n)$，因此 $r=1$. 这表明

$$\langle g\rangle\cap\langle h\rangle=\{e\},$$

又 gh 的阶为 k，故

$$(gh)^k=g^kh^k=e,$$

从而

$$g^k=(h^{-1})^k\in\langle g\rangle\cap\langle h\rangle=\{e\}.$$

于是

$$m|k,$$

同理

$$h^k=(g^{-1})^k\in\langle h\rangle\cap\langle g\rangle=\{e\},$$

故

$$n|k,$$

因为 $(m,n)=1$，所以

$$mn|k,$$

从而 $k=mn$.

我们知道，循环群的阶与其生成元的阶相同，再由定理 2.4.3，不难得到下面结论.

定理 2.4.4 设 $G=\langle a\rangle$ 是循环群.

(1) 若 G 是无限阶群，则它的生成元只有两个 a 和 a^{-1}.

(2) 若 G 是 n 阶群，则它有 $\varphi(n)$ 个生成元. 对于每个不超过 n 且与 n 互素的正整数 r，a^r 都是 G 的生成元.

定理 2.4.5 设 $G=\langle a\rangle$ 是循环群，则

(1) G 的子群也是循环群；

(2) 如果 G 是无限循环群，除了 $\{e\}$ 以外，G 的其他子群都是无限循环群；

(3) 如果 G 是 n 阶循环群，那么对于 n 的每个正因子 r，G 有且只有一个 r 阶循环群.

证明 (1) 设 G_1 是 G 的子群，令

$$k=\min\{m\in Z^+\mid a^m\in G_1\},$$

下面我们证明 $G_1=\langle a^k\rangle$.

事实上 $\langle a^k\rangle\subseteq G_1$. 又任取 $a^r\in G_1$，其中 $r\in Z^+$，则 $r\geqslant k$. 设

$$r=nk+s,0\leqslant s<k.$$

如果 $s\neq0$，则 $a^r=a^{nk}\cdot a^s\in G_1$，而 $a^{nk}\in G_1$，故

$$a^s=(a^{nk})^{-1}\cdot a^r\in G_1,$$

与 k 的选取矛盾.

因此 $s=0$，所以 $r=nk$. 因此 $a^r\in\langle a^k\rangle$，故

$$G_1\subseteq\langle a^k\rangle,$$

因此 $G_1=\langle a^k\rangle$.

(2) 设 G 是无限循环群，H 是它的子群. 如果 $H\neq\{e\}$，即 H 中存在非单位元的元素，设 a^m 是 H 中最小正方幂元. 由(1)的证明得知，$H=\langle a^m\rangle$. 假设 H 的阶是 t，则 a^m 的阶也是 t，即有

$$(a^m)^t=a^{mt}=e.$$

这与 a 是无限阶元相矛盾.

(3) 设 $G=\langle a\rangle$ 是 n 阶循环群，对于 n 的正因子 d，易见

$$H=\langle a^{n/d}\rangle$$

是 G 的 d 阶子群. 下面证明唯一性.

假设 $K=\langle a^m\rangle$ 也是 G 的 d 阶子群，其中 a^m 是 K 中最小正方幂元. 则 $(a^m)^d=e$，再由性质 2.1.6，得到 $n\mid md$，从而

$$\frac{n}{d}\Big| m.$$

令 $m=\frac{n}{d}l$，其中 l 是整数，则有

$$a^m=a^{\frac{n}{d}l}=(a^{\frac{n}{d}})^l\in H.$$

从而证明了 $K\subseteq H$.

又由于 K 和 H 都是 d 阶群，因此 $K=H$.

从这个定理得出，对于 n 阶循环群，只要找出 n 的所有正因子，就可以求出它的所有子群.

例 2.4.3　求下述循环群 G 的所有子群和所有生成元.

(1) $G=\langle a\rangle$ 为无限循环群；

(2) G 为模 15 剩余类加群 Z_{15}；

(3) G 为 12 阶循环群 $\langle a\rangle$；

解　(1) G 的生成元为 a,a^{-1}.

子群为

$\langle e\rangle=\{e\}$

$\langle a\rangle=\{a\ \ ^{1}\}=G$

$\langle a^i\rangle=\{a^{-i}\}=\{e,a^{\pm i},a^{\pm 2i},a^{\pm 3i},\cdots\},\quad i\in Z$

(2) 小于 15 并与 15 互素的正整数是 1,2,4,7,8,11,13,14.

Z_{15}的生成元是:1,2,4,7,8,11,13,14.

15 的正因子是 1,3,5,15. 所以 Z_{15}的 4 个子群为

1 阶子群$\langle[0]\rangle=\{[0]\}$;

3 阶子群$\langle[5]\rangle=\{[0],[5],[10]\}$;

5 阶子群$\langle[3]\rangle=\{[0],[3],[6],[9],[12]\}$;

15 阶子群为 Z_{15}.

(3) 与 12 互素的元为 1,5,7,11. 所以 G 的生成元为 a,a^5,a^7,a^{11}.

12 的正因子是 1,2,3,4,6,12. 所以 G 的 6 个子群为

1 阶子群$\langle e\rangle=\{e\}$;

2 阶子群$\langle a^6\rangle=\{e,a^6\}$;

3 阶子群$\langle a^4\rangle=\{e,a^4,a^8\}$;

4 阶子群为 $\langle a^3\rangle=\{e,a^3,a^6,a^9\}$;

6 阶子群为 $\langle a^2\rangle=\{e,a^2,a^4,a^6,a^8,a^{10}\}$;

12 阶子群为 G.

2.5 正规子群,商群与同态定理

正规子群对刻画群的性质起着重要作用. 群关于其正规子群的陪集全体也构成群,即商群. 进一步,我们研究群和其商群的关系.

2.5.1 正规子群

定义 2.5.1 群 G 的子群 N 称为 G 的正规子群(或不变子群),如果 $\forall a\in G$,

$$aN=Na,$$

此时称 $aN(Na)$为 N 的一个陪集. 若 N 是 G 的正规子群,记为 $N\lhd G$.

值得注意的是这里 $aN=Na$,是指两个集合相等,并不是 $\forall n\in N$,有 $an=na$.

例如:G 和 $\{e\}$都是 G 的正规子群,$C(G)=\{g\in G|\ \forall a\in G,ag=ga\}$是 G 的正规子群,Abel 群的任意子群都是正规子群.

定理 2.5.1 设 H 是群 G 的子群,则下列条件等价:

(1) $H \lhd G$;

(2) $gHg^{-1}=H, \forall g\in G$;

(3) $g_1Hg_2H=g_1g_2H, \forall g_1,g_2\in G$.

证明　(1)⇒(2). 已知 $H\lhd G$,即 $\forall g\in G, gH=Hg$,于是 $\forall g\in G$,

$$(gH)g^{-1}=(Hg)g^{-1}=H(gg^{-1})=H.$$

(2)⇒(3). 已知 $\forall g\in G, gHg^{-1}=H$. 于是 $\forall g_1,g_2\in G$,

$$g_1g_2H=(g_1e)g_2H\subseteq g_1Hg_2H.$$

又任取 $h_1,h_2\in H$,

$$g_1h_1g_2h_2=g_1g_2(g_2^{-1}h_1g_2)h_2,$$

因为 $g_2^{-1}Hg_2=H$,

故 $(g_2^{-1}h_1g_2)h_2\in H$,从而

$$g_1h_1g_2h_2\in g_1g_2H,$$

即 $g_1Hg_2H\subset g_1g_2H$,因此 $g_1g_2H=g_1Hg_2H$.

(3)⇒(1). 已知 $\forall g_1,g_2\in G, g_1Hg_2H=g_1g_2H$. 于是

$$\forall g\in G, h\in H, eHgH=HgH=egH=gH,$$

$hg=hge\in HgH=gH$,故 $Hg\subseteq gH$.

同理 $Hg^{-1}\subseteq g^{-1}H$,即 $gH\subseteq Hg$,

故 $gH=Hg, H\lhd G$.

定义 2.5.2　若群 G 没有非平凡的正规子群,则称 G 为单群.

素数阶的群一定是单群,$A_n(n\geqslant 5)$是非 Abel 单群(证明略去). 有限单群是群论的一个重要研究内容,最基本的问题是有限单群的分类,即在同构意义下有多少类有限单群,这个问题直到 20 世纪 80 年代才得以解决.

2.5.2　商群

设 N 为 G 的正规子群,N 的全体陪集构成的集合为 S. 在 S 中定义运算

$$aN\cdot bN=(ab)N.$$

首先证明这是 S 的代数运算,即运算结果与陪集的代表元无关,亦即若 $a_1N=a_2N$, $b_1N=b_2N$,则 $(a_1b_1)N=(a_2b_2)N$.

事实上,由 $a_1N=a_2N, b_1N=b_2N$,可知 $a_1^{-1}a_2=n_1\in N, b_1^{-1}b_2=n_2\in N$,因此

$$(a_1b_1)^{-1}(a_2b_2)=b_1^{-1}a_1^{-1}a_2b_2=n_2b_2^{-1}n_1b_2.$$

因为 N 为 G 的正规子群,由定理 2.5.1 可知,$b_2^{-1}Nb_2=N$,所以

$$(a_1b_1)^{-1}(a_2b_2)=b_1^{-1}a_1^{-1}a_2b_2=n_2b_2^{-1}n_1b_2\in N,$$

故 $a_1b_1N=a_2b_2N$.

在 S 中定义了上述代数运算后，可验证 S 关于该运算构成群.

首先，S 对该运算封闭；其次 $\forall a,b,c\in G$，

$$(aNbN)cN=(ab)NcN=[(ab)c]N,$$

$$aN(bNcN)=aN(bcN)=[a(bc)]N.$$

因为 $(ab)c=a(bc)$，故该运算适合结合律.

S 中的元 $eN=N$，而 $\forall a\in G$，$(aN)N=aN$，$N(aN)=aN$，即 N 是单位元.

$\forall aN\in S$，$a^{-1}N$ 是 aN 的逆元，这是因为

$$aNa^{-1}N=(aa^{-1})N=N,$$

$$(a^{-1}N)(aN)=(a^{-1}a)N=N.$$

总之，S 关于上述运算构成群.

定义 2.5.3 设 N 是 G 的正规子群，N 的全体陪集关于运算

$$(aN)(bN)=(ab)N$$

构成一个群，称为 G 对 N 的商群，记为，G/N.

2.5.3 群同态定理

定理 2.5.2 群 G 同它的每一个商群 G/N 同态（即存在群 G 到 G/N 的满同态映射）.

证明 定义映射 $f:G\to G/N$ 为

$$f(g)=gN,\quad \forall g\in G.$$

显然 f 是从 G 到 G/N 的满射，且

$$f(g_1g_2)=g_1g_2N=g_1Ng_2N=f(g_1)f(g_2),$$

即 f 是同态映射.

上述从 G 到 G/N 的同态映射 f 称为自然同态，一般记为 π，有

$$\pi(g)=gN,\quad \forall g\in G.$$

定义 2.5.4 设 f 是从群 G_1 到群 G_2 的同态，G_2 的单位元 e_2 在 f 之下的所有原象的集合称为 f 的核，记为 $\mathrm{Ker}(f)$，即

$$\mathrm{Ker}(f)=\{a\mid a\in G_1, f(a)=e_2\}.$$

定理 2.5.3 （群同态基本定理）设 f 是从群 G 到群 $\tilde{G}$ 的同态满射，则

(1) $\mathrm{Ker}(f)\lhd G$;

(2) $G/\mathrm{Ker}(f)\cong\widetilde{G}$.

证明　(1) 由核的定义,$\mathrm{Ker}(f)=\{g\in G\mid f(g)=\tilde{e},\tilde{e}$ 是 $\widetilde{G}$ 的单位元$\}$.

因为 $f(e)=\tilde{e}$,e 为 G 的单位元,即 $e\in\mathrm{Ker}(f)$. 这说明 $\mathrm{Ker}(f)$是非空集合.

$\forall g_1,g_2\in\mathrm{Ker}(f)$,$f(g_1g_2^{-1})=f(g_1)f(g_2^{-1})=f(g_1)[f(g_2)]^{-1}=\tilde{e}\tilde{e}=\tilde{e}$,即有 $g_1g_2^{-1}\in\mathrm{Ker}(f)$,故 $\mathrm{Ker}(f)$是 G 的子群.

任取 $n\in\mathrm{Ker}(f)$,$\forall a\in G$,

$$f(ana^{-1})=f(a)f(n)f(a^{-1})=f(a)f(a^{-1})=f(aa^{-1})=f(e)=\tilde{e},$$

即 $ana^{-1}\in\mathrm{Ker}(f)$,所以 $a\mathrm{Ker}(f)a^{-1}\subseteq\mathrm{Ker}(f)$.

同理有 $a^{-1}\mathrm{Ker}(f)a\subseteq\mathrm{Ker}(f)$,即 $\mathrm{Ker}(f)\subseteq a\mathrm{Ker}(f)a^{-1}\subseteq\mathrm{Ker}(f)$.

因此 $a\mathrm{Ker}(f)a^{-1}=\mathrm{Ker}(f)$,这说明 $\mathrm{Ker}(f)$是 G 的正规子群.

(2) 定义映射 $\Phi:G/\mathrm{Ker}(f)\to\widetilde{G}$ 为

$$\Phi(gN)=f(g),\forall g\in G.\text{(记 }\mathrm{Ker}(f)=N\text{)}$$

先说明上述 Φ 是从 G/N 到 $\widetilde{G}$ 的映射,即与陪集 gN 的代表元无关.

事实上,若 $g_1N=g_2N$,则 $g_1^{-1}g_2\in N$,$f(g_1^{-1}g_2)=f(g_1^{-1})f(g_2)=[f(g_1)]^{-1}f(g_2)=\tilde{e}\tilde{e}=\tilde{e}$,因此 $f(g_1)=f(g_2)$,故 Φ 是从 G/N 到 $\widetilde{G}$ 的映射.

因为 f 是满射,所以 $\widetilde{G}=f(G)$,从而 Φ 是满射;若 $\Phi(g_1N)=\Phi(g_2N)$,则 $f(g_1)=f(g_2)$,$f(g_1^{-1}g_2)=\tilde{e}$,$g_1^{-1}g_2\in N$,故 $g_1N=g_2N$. 总之 Φ 是从 G/N 到 $\widetilde{G}$ 的一一映射.

最后证明 Φ 是同态映射. $\forall g_1,g_2\in G$,

$$\Phi(g_1Ng_2N)=\Phi(g_1g_2N)=f(g_1g_2)=f(g_1)f(g_2)=\Phi(g_1N)\Phi(g_2N).$$

定理 2.5.2 和定理 2.5.3 说明,群 G 与它的任意商群同态,且只能与它的商群同态. 一般来说,群 G 的同态象 $f(G)$与 G 并不完全相同,但 $f(G)$却与 G 的某个商群 G/N 在同构意义下完全相同.

定理 2.5.4　设群 G_1 与群 G_2 同态(即存在从 G_1 到 G_2 的同态满射 f),则在这个同态满射 f 之下:

(1) G_1 的子群 H_1 的象 $f(H_1)$是 G_2 的子群;

(2) G_1 的正规子群 N_1 的象 $f(N_1)$是 G_2 的正规子群;

(3) G_2 的子群 H_2 的原象 H_1 是 G_1 的子群;

(4) G_2 的正规子群 H_2 的原象 N_1 是 G_1 的正规子群.

证明　(1) 显然 $f(H_1)=\{f(a)\mid a\in H_1\}$是群 $G_2=f(G_1)$的非空子集.

任取 $f(a),f(b)\in f(H_1)$,其中 $a,b\in H_1$. 因为 H_1 是 G_1 的子群,所以 $ab^{-1}\in H_1$. 于是 $f(a)[f(b)]^{-1}=f(a)f(b^{-1})=f(ab^{-1})\in f(H_1)$,因此 $f(H_1)$是 $G_2=f(G_1)$的子群.

(2) 由(1)已知 $f(N_1)$是 $G_2=f(G_1)$的子群. 任取 $f(a)\in G_2=f(G_1)$,其中 $a\in G_1$. 因为 N_1 是 G_1 的正规子群,所以 $aN_1=N_1a$. 于是

$$f(a)f(N_1)=f(aN_1)=f(N_1a)=f(N_1)f(a),$$

所以 $f(N_1)$是 $G_2=f(G_1)$的正规子群.

(3) 显然 $H_1=\{a\in G_1\,|\,f(a)\in H_2\}$是群 G_1 的非空子集.

任取 $a,b\in H_1$,则 $f(a),f(b)\in H_2$. 因为 H_2 是 G_2 的子群,所以

$$f(a)[f(b)]^{-1}=f(a)f(b^{-1})=f(ab^{-1})\in H_2.$$

于是 $ab^{-1}\in H_1$,因此 H_1 是 G_1 的子群.

(4) 由(3)已知 N_1 是 G_1 的子群. 任取 $a\in G_1$,因为 N_2 是 $G_2=f(G_1)$的正规子群,所以

$$f(a)N_2[f(a)]^{-1}=f(a)N_2f(a^{-1})=N_2.$$

于是 $\forall n_1\in N_1, f(a)f(n_1)f(a^{-1})=f(an_1a^{-1})\in N_2$,因此 $an_1a^{-1}\in N_1$,即 $aN_1a^{-1}\subseteq N_1$,同理可证 $a^{-1}N_1a\subseteq N_1$,即 $N_1\subseteq aN_1a^{-1}$,所以 $aN_1a^{-1}=N_1$, N_1 是 G_1 的正规子群.

2.6* 群在集合上的作用

考虑同态是研究群之间关系的基本手段. 为了研究一个群 G,我们希望有一些理想的"样板"群作为标准,然后通过研究群 G 到样板群的各种同态来把握 G 的特性. 变换群是一类理想的样板群. 一个群 G 到变换群的同态叫做 G 的置换表示,本节的目的是介绍群的置换表示理论的一些基本知识.

定义 2.6.1 设 X 是一个非空集合,$S(X)$是 X 上的全变换群(即 X 的全体一一变换构成的群). 群 G 到 $S(X)$的每个同态 $f:G\to S(X)$称为群 G 在集合 X 上的一个置换表示. 如果 f 是单同态,则称 f 是忠实表示.

如果 f 是群 G 的一个置换表示,则群 G 借助于 f 作用在集合 X 上,也就是说,元素 $g\in G$在集合 X 上的作用看成是置换 $f(g)$. $\forall a\in X$,定义 $g(a)=f(g)(a)$,若 f 是忠实表示,群 G 借助于 f 作用在集合 X 上,则当且仅当 $g=e$ 时,才有 $\forall x\in X, g(x)=x$. 此时称 G 在 X 上的作用是有效的.

例 2.6.1　设 G 是群，取 $X=G$，作如下映射 $\rho:G\to S(G)$，使得 $\rho(g)(a)=ga$，$\forall g,a\in G$，也就是说，对于 $g\in G$，$\rho(g)$ 是集合 G 上如下的一一变换：它将 G 的每个元素 a 变成 ga（由群 G 上的消去律可知 $\rho(g)$ 是 G 上的一一变换）. 由于 $[\rho(g_1)\rho(g_2)](a)=\rho(g_1)[\rho(g_2)(a)]=\rho(g_1)(g_2a)=g_1g_2a=\rho(g_1g_2)(a)$，因此 ρ 是群的同态，因此 ρ 是群 G 在集合 G 上的一个置换表示，称为群 G 的左正则表示.

$g\in \mathrm{Ker}(\rho)\Leftrightarrow \forall a\in G, g(a)=ga=a$，故 $g=e$，因此 ρ 是单同态，左正则表示是忠实的，群 G 借助于左正则表示 ρ 作用在集合 G 上，相当于是 $\forall g,x\in G, g(x)=gx$，这种作用称为左平移作用.

类似，$\tau:G\to S(G)$，$\tau(g)(a)=ag^{-1}$，$\forall g,a\in G$，则 τ 也是群 G 在集合 G 上的一个置换表示，称为群 G 的右正则表示. 群 G 借助于右正则表示作用在集合 G 上，相当于是 $\forall g,x\in G, g(x)=xg^{-1}$，这种作用称为右平移作用.

例 2.6.2　设 H 为群 G 的子群，取 X 为 H 在 G 中全体左陪集的集合. 定义 $\rho:G\to S(X)$ 如下：$\forall g\in G, \rho(g)(aH)=gaH, \forall aH\in X$. 也就是说，对于 $g\in G$，$\rho(g)$ 是集合 X 上如下的对应关系：它将 X 的每个元素 aH 变成 gaH.

(1) 首先验证 $\rho(g)$ 是 X 上的一一变换.

首先，任取 $a_1,a_2\in G$，若 $a_1H=a_2H$，由性质 1.4.2 可知 $a_1^{-1}a_2\in H$，于是 $(ga_1)^{-1}(ga_2)=a_1^{-1}a_2\in H$，由性质 1.4.2 得 $ga_1H=ga_2H$. 这说明 $\rho(g)$ 与左陪集的代表元无关，是 X 上的变换.

其次，$\forall aH\in X, \rho(g)(g^{-1}aH)=aH$，即 $\rho(g)$ 是满射；$\forall a_1,a_2\in G$，若 $ga_1H=ga_2H$，则 $(ga_1)^{-1}(ga_2)=a_1^{-1}a_2\in H$，于是 $a_1H=a_2H$，即 $\rho(g)$ 是单射. 总之 $\rho(g)$ 是 X 上的一一变换.

(2) 由于 $\forall aH\in X$，

$$[\rho(g_1)\rho(g_2)](aH)=\rho(g_1)[\rho(g_2)(aH)]=\rho(g_1)(g_2aH)=g_1g_2aH=\rho(g_1g_2)(aH),$$

即 $\rho(g_1)\rho(g_2)=\rho(g_1g_2)$，$\forall g_1,g_2\in G$，因此 ρ 是群的同态.

由(1)、(2)可知 ρ 是群 G 在集合 X 上的一个置换表示. 群 G 借助于 ρ 作用在集合 X 上，相当于是 $\forall g\in G, \forall aH\in X, g(aH)=gaH$. 当 $H=\{e\}$ 时，这个作用恰好是 G 在 G 上的左平移作用.

例 2.6.3　设 G 是一个群，取 $X=G$，定义 $\rho:G\to S(G)$ 如下：$\forall g\in G, \rho(g)(x)=gxg^{-1}, \forall x\in G$. 也就是说，对于 $g\in G$，$\rho(g)$ 是集合 G 上如下的一一变换：它将 G 的每个元素 x 变成 gxg^{-1}（由群 G 上的消去律可知 $\rho(g)$ 是 G 上的一一变换）. 又

$$[\rho(g_1)\rho(g_2)](x)=\rho(g_1)[\rho(g_2)(x)]=\rho(g_1)(g_2xg_2^{-1})$$
$$=g_1(g_2xg_2^{-1})g_1^{-1}=(g_1g_2)x(g_1g_2)^{-1}=\rho(g_1g_2)(x)$$

即 $\rho(g_1)\rho(g_2)=\rho(g_1g_2)$，$\forall g_1,g_2\in G$.

因此 ρ 是群的同态，从而 ρ 是群 G 在集合 G 上的一个置换表示. 群 G 借助于 ρ 作用在集合 G 上，相当于是 $\forall g\in G, g(x)=gxg^{-1}$，$\forall x\in G$. 这种作用称为群 G 在集合 G 上的伴随作用.

定义 2.6.2 设群 G 作用在集合 X 上，$\forall x\in X$，称 X 中的子集 $O_x=\{g(x)\mid g\in G\}$ 为 x 的轨道.

下面证明：$O_x=O_y$ 或 $O_x\cap O_y=\Phi$，$\forall x,y\in G$. 这说明 $X=\bigcup\limits_{x\in X}O_x$ 是集合 X 的一个分划.

证明 在 X 中定义关系 R：$\forall x,y\in X, xRy\Leftrightarrow\exists g\in G$，使 $y=g(x)$. 则 $\forall x\in X$，xRx；$\forall x,y\in X$，若 xRy，即 $\exists g\in G$，使 $y=g(x)$，则

$$g^{-1}(y)=g^{-1}[g(x)]=(g^{-1}g)(x)=e(x)=x,$$

因此 yRx；$\forall x,y,z\in X$，若 xRy, yRz，即 $\exists g_1,g_2\in G$，使 $y=g_1(x), z=g_2(y)$，则 $z=g_2[g_1(x)]=(g_1g_2)(x)$，因此 xRz，这说明 R 是 X 中的等价关系，O_x 正好是 x 所在的等价类. 因此 $\forall x,y\in G, O_x=O_y$ 或 $O_x\cap O_y=\Phi$.

定义 2.6.3 设群 G 作用在集合 X 上，则 $\forall x\in X, G_x=\{g\in G\mid g(x)=x\}$ 是 G 的一个子群，称为元素 a 的固定子群(或迷向子群).

定理 2.6.1（轨道公式） 设有限群 G 作用在集合 X 上，则 $\forall x\in X$，$|G|=|G_x|\,|O_x|$.

证明 $\forall x\in X$，作 G 对子群 G_x 的陪集分解，$G=g_1G_x\cup g_2G_x\cup\cdots\cup g_nG_x$，$n=[G:G_x]$. 令 $g_i(x)=x_i$，$1\leqslant i\leqslant n$. 对每个 $g\in G$，有唯一的 $i(1\leqslant i\leqslant n)$，使得 $g\in g_iG_x$. 令 $g=g_ih$，$h\in G_x$，则 $g(x)=(g_ih)x=g_i[h(x)]=g_i(x)=x_i$，又 $x_i=x_j\Leftrightarrow g_i(x)=g_j(x)\Leftrightarrow g_j^{-1}[g_i(x)]=x\Leftrightarrow g_j^{-1}g_i\in G_x\Leftrightarrow g_jG_x=g_iG_x\Leftrightarrow i=j$. 从而 $x_1,x_2,\cdots,x_n$ 两两相异，$O_x=\{x_1,x_2,\cdots,x_n\}$ 是 n 元集合. 即 $|O_x|=n=[G:G_x]=\dfrac{|G|}{|G_x|}$.

定义 2.6.4 设 G 是一个群，$g\in G$，g 在伴随作用下的轨道 $O_g=\{aga^{-1}\mid a\in G\}$ 称为以 g 为代表的共轭类. 若 $h\in O_g$，则称 h 与 g 共轭(即存在 $a\in G$，使 $h=aga^{-1}$).

2.7* Sylow 子群

Sylow 子群是有限群理论的重要内容，它在群的结构研究中有重要的应用. 建立 Sy-

low 子群理论的途径是多样的，其中之一是采用群在集合上的作用来建立这些理论. 本节不加证明地给出这些理论及其简单应用.

设 G 是有限群，$a\in G$. 分别用符号 $|G|$ 和 $|a|$ 来表示 G 的阶及元素 a 的阶（也称为 a 的周期）. 由 Lagrange 定理可知，对群的任一子群 H，有 $|H|$ 整除 $|G|$. 反过来的逆命题是不成立的，但有下面的结论.

定理 2.7.1 设 G 是有限群，p 是素数，p 整除 $|G|$. 则 G 中存在元素 a，使 $|a|=p$.

由定理 2.7.1 可知，当素数 p 整除 $|G|$ 时，G 中存在阶数为 p 的子群. 进一步，可以给出下面的概念和结论.

定义 2.7.1 设 G 是有限群，p 是素数. $|G|=p^r m$，$(p,m)=1$. 称 G 的阶数为 p^r 的子群为 G 的 Sylow p-子群.

下面介绍两个定理.

定理 2.7.2 设 G 是一个阶为 $p^l m$ 的群，其中 p 为素数，$l\in Z^+$，$(p,m)=1$. 则对任何 $k\leqslant l(k\in Z^+)$，G 中必有 p^k 阶子群.

定理 2.7.3 设 G 是一个阶为 $p^l m$ 的群，其中 p 为素数，$l\in Z^+$，$(p,m)=1$. 如果 G 中 Sylow p-子群的个数为 k，则：

(1) $k\,|\,m$，$k\equiv 1(\bmod p)$；

(2) 当且仅当 $k=1$ 时，G 的 Sylow p-子群 P 满足 $P\lhd G$.

下面举例说明上面定理的应用.

例 2.7.1 设 $|G|=15$. 因为 $15=3\times 5$，G 的 Sylow p-子群（$p=3$）的个数 $k_3=3l+1$，且 $k_3\,|\,15$，故 $k_3=1$. G 的 Sylow p-子群（$p=5$）的个数 $k_5=5l+1$，且 $k_5\,|\,15$，故 $k_5=1$. 即 G 含有两个正规子群 C_3，C_5（C_n 表示 n 阶循环群）. 于是 $G=C_3\times C_5$. 因此从同构的意义来说，阶数为 15 的群只有一个，就是 15 阶循环群.

例 2.7.2 求证：148 阶群 G 不是单群.

证明 $148=2^2\times 37$，故 G 中有 Sylow p-子群（$p=37$），其个数 $k_{37}=37l+1$，且 $k_{37}\,|\,148$. 因此 $k_{37}=1$，即 G 只有一个 37 阶子群，它是正规子群，故 G 不是单群.

2.8* 有限 Abel 群的结构

2.8.1 群的直积

定义 2.8.1 设 G_1，G_2 是群，集合 $G_1\times G_2$ 关于乘法 $(a_1,a_2)(b_1,b_2)=(a_1b_1,a_2b_2)$ 构

成群(请读者自行验证),称之为 G_1,G_2 的直积,记为 $G_1\times G_2$.

设 G_1,G_2 的单位元分别为 e_1,e_2,则 $G_1\times G_2$ 的单位元为 (e_1,e_2),(a,b) 的逆元为 (a^{-1},b^{-1}). 当 G_1,G_2 均为有限群时,$G_1\times G_2$ 也是有限群,且 $|G_1\times G_2|=|G_1||G_2|$. 当 G_1,G_2 都是 Abel 群时,$G_1\times G_2$ 也是 Abel 群.

类似可定义 n 个群 $G_1,G_2,\cdots,G_n$ 的直积 $G_1\times G_2\times\cdots\times G_n$.

例 2.8.1 设 C_n 表示 n 阶循环群,则 $C_3\times C_5=C_{15}$. 因为 $C_3\times C_5$ 是 15 阶群,只需证明 $C_3\times C_5$ 中存在阶为 15 的元素即可. 设 $C_3=(a)$,$C_5=(b)$,则 (a,b) 的阶 k 满足 $k\mid 15$,易见 $k\neq 1,3,5$,故 $k=15$.

一般的,设 p,q 是互异的素数,类似可证 $C_p\times C_q=C_{pq}$. 读者可进一步证明:若正整数 r,s 互素,则 $C_r\times C_s=C_{rs}$.

2.8.2 有限 Abel 群的结构

定理 2.8.1 设 G 是有限 Abel 群,$|G|=p_1^{k_1}p_2^{k_2},\cdots,p_n^{k_n}$,其中 $p_1,p_2,\cdots,p_n$ 是两两不同的素数,$k_1,k_2,\cdots,k_n$ 是正整数. 则 $G=S_{p_1}\times S_{p_2}\times\cdots\times S_{p_n}$,其中 S_{p_i} 是 G 的 Sylow p_i-子群,$1\leqslant i\leqslant n$.

定义 2.8.2 如果群 G 中不存在真子群 G_1,G_2,使 $G=G_1\times G_2$,则称群 G 是不可分解的. 进一步,有下面的结论.

定理 2.8.2 (初等因子定理)任一有限 Abel 群 $G(G\neq\{e\})$ 均可表为不可分解群的直积:$G=G_1\times G_2\times\cdots\times G_s(*)$,其中 G_i 是阶数为素数幂 $p_i^{\alpha_i}$ 的循环群. 称 $\{p_1^{\alpha_1},p_2^{\alpha_2},\cdots,p_s^{\alpha_s}\}$ 为分解 $(*)$ 的初等因子组. 若 G 另有性质相同的分解 $G=K_1\times K_2\times\cdots\times K_r$,其中 $K_i\neq\{e\}(1\leqslant i\leqslant r)$ 是阶数为素数幂 $q_i^{\beta_i}$ 的循环群,则 $r=s$,$\{p_1^{\alpha_1},p_2^{\alpha_2},\cdots,p_s^{\alpha_s}\}=\{q_1^{\beta_1},q_2^{\beta_2},\cdots,q_r^{\beta_r}\}$.

由此可见,两个有限 Abel 群同构的充要条件是它们有相同的初等因子组.

例 2.8.2 列举所有的 8 阶 Abel 群.

解 因为 $8=2^3$,故初等因子组有以下几种可能:$\{2^3\}$;$\{2^2,2\}$;$\{2,2,2\}$. 可见 8 阶群从同构的意义来看只有三个:C_8;$C_4\times C_2$;$C_2\times C_2\times C_2$.

例 2.8.3 列举所有的 36 阶 Abel 群.

解 因为 $36=2^2\times 3^2$,故初等因子组有以下几种可能:$\{2^2,3^2\}$;$\{2,2,3^2\}$;$\{2^2,3,3\}$;$\{2,2,3,3\}$. 可见 36 阶群从同构的意义来看只有四个:C_{36};$C_2\times C_{18}$;$C_3\times C_{12}$;$C_6\times C_6$.

定理 2.8.3 (不变因子定理)任一有限 Abel 群均可表为循环群的直积:$G=H_1\times H_2\times\cdots\times H_r(**)$,其中 $H_i\neq\{e\}(1\leqslant i\leqslant r)$ 是循环群,其阶数 h_i 具有性质 $h_i\mid h_{i+1}(1\leqslant$

$i \leqslant r-1$). $\{h_1, h_2, \cdots, h_r\}$称为分解($**$)的不变因子组.若 G 另有性质相同的分解 $G=K_1 \times K_2 \times \cdots \times K_s$,其中 $K_i \neq \{e\}(1 \leqslant i \leqslant s)$是 k_i 阶循环群,且 $k_i \mid k_{i+1}(1 \leqslant i \leqslant s-1)$,则 $r=s, k_i=h_i(1 \leqslant i \leqslant r)$.

由此可见:两个有限群同构的充要条件是它们有相同的不变因子组.

例 2.8.4　设 p 为素数,则 p^4 阶 Abel 群的初等因子组有以下几种可能:$\{p^4\}$;$\{p^3, p\}$;$\{p^2, p^2\}$;$\{p^2, p, p\}$;$\{p, p, p, p\}$.从同构的意义来看 p^4 阶 Abel 群有 5 个:C_{p^4};$C_{p^3} \times C_p$;$C_{p^2} \times C_{p^2}$;$C_{p^2} \times C_p \times C_p$;$C_p \times C_p \times C_p \times C_p$. 因此 p^4 阶 Abel 群的不变因子组为$\{p^4\}$;$\{p, p^3\}$;$\{p^2, p^2\}$;$\{p, p, p^2\}$;$\{p, p, p, p\}$.

例 2.8.5　由例 2.8.3 已知 36 阶 Abel 群从同构的意义来看只有四个:C_{36};$C_2 \times C_{18}$;$C_3 \times C_{12}$;$C_6 \times C_6$.因此 36 阶 Abel 群的不变因子组为:$\{36\}$;$\{2,18\}$;$\{3,12\}$;$\{6,6\}$.

2.9　群在密码体制中的应用

信息安全是信息时代最为关注的问题之一,密码学是信息安全的核心技术.密码学的加密体制按密钥的特性分为私钥密码(对称密码)体制和公钥密码(非对称密码)体制.

公钥密码算法是以非对称的形式使用两个密钥,两个密钥的使用对保密性、密钥分配、认证等都有着深刻的意义.1976 年 W. Diffie 和 M. Hellman 提出了公钥密码系统的观点,在 1977 年 Rivest,Shamir,Adleman 给出了第一个比较完善的公钥密码算法,这就是著名的 RSA 算法.它的特点是采用两个相关密钥将加密和解密分开,它的安全性是基于分解大整数的困难性.

具体的算法简述为:

(1) 密钥的产生

① 选两个保密的大素数 p 和 q.

② 计算 $n=pq, \varphi(n)=(p-1)(q-1)$,其中 $\varphi(n)$是 n 的欧拉函数值.

③ 选整数 e,满足 $1<e<\varphi(n)$,且 $\gcd(\varphi(n), e)=1$.

④ 计算 d,满足 $de \equiv 1 \pmod{\varphi(n)}$,即 d 是 e 在模 $\varphi(n)$下的乘法逆元,因 e 与 $\varphi(n)$互素,它的乘法逆元一定存在.

⑤ 以$\{e, n\}$为公开密钥,$\{d, p, q\}$为秘密密钥.

(2) 加密

首先将明文比特串分组,使得每个分组对应的十进制数小于 n,即分组长度小于 $\log_2 n$.

然后对每个明文分组 m,作加密运算:$c \equiv m^e \pmod n$.

(3) 解密

对密文分组的解密运算为 $m \equiv c^d \pmod n$.

下面证明 RSA 算法中解密过程的正确性.

证明 由加密过程知 $c \equiv m^e \pmod n$,所以

$$c^d \equiv m^{ed} \equiv m^{1 \bmod \phi(n)} = m^{k\phi(n)+1} \pmod n$$

下面分两种情况:

① m 与 n 互素,则由 Euler 定理得

$$m^{\varphi(n)} \equiv 1 \pmod n, \quad m^{k\varphi(n)} \equiv 1 \pmod n, \quad m^{k\varphi(n)+1} \equiv m \pmod n,$$

即 $c^d \equiv m \pmod n$.

② $\gcd(m,n) \neq 1$,说明 m 是 p 的倍数或 q 的倍数,不妨设 $m=tp$,其中 t 为正整数. 此时必有 $\gcd(m,q)=1$,否则 m 也是 q 的倍数,从而是 pq 的倍数,与 $m<n=pq$ 矛盾. 由 $\gcd(m,q)=1$ 及 Euler 定理得 $m^{\varphi(q)} \equiv 1 \bmod q$,所以

$$m^{k\phi(q)} \equiv 1 \pmod q, [m^{k\phi(q)}]^{\phi(p)} \equiv 1 \pmod q, m^{k\phi(n)} \equiv 1 \pmod q.$$

因此存在整数 r,使得 $m^{k\varphi(n)} = 1 + rq$,两边同乘以 $m=tp$ 得

$$m^{k\phi(n)+1} = m + rtpq = m + rtn,$$

即 $m^{k\phi(n)+1} = m \pmod n$,所以 $c^d \equiv m \pmod n$.

例 2.9.1 选 $p=7, q=17$. 求 $n=p\times q=119$, $\varphi(n)=(p-1)(q-1)=96$.

解 取 $e=5$,满足 $1<e<\varphi(n)$,且 $\gcd(\varphi(n),e)=1$.

确定满足 $d\cdot e=1 \pmod{96}$ 且小于 96 的 d,因为 $77\times 5=385=4\times 96+1$,所以 d 为 77.

因此公开钥为{5,119},秘密钥为{77,7,17}.

设明文 $m=19$,则由加密过程得密文为

$$c \equiv 19^5 \equiv 2476099 \equiv 66 \pmod{119}.$$

解密为

$$66^{77} \equiv 19 \pmod{119}.$$

习　　题

1. 设 $\mathbf{R}$ 表示全体实数的集合，$\mathbf{R}^*$ 表示全体非零实数. 在 $\mathbf{R}^*\times\mathbf{R}$ 中定义运算如下：$(a,b)(c,d)=(ac,ad+b)$，$\forall (a,b),(c,d)\in\mathbf{R}^*\times\mathbf{R}$，试证 $\mathbf{R}^*\times\mathbf{R}$ 是群.

2. 令 Ω 是任意一个集合，G 是一个群，Ω^G 是 Ω 到 G 的所有映射的集合. 对任意两个映射 $f,g\in\Omega^G$，定义乘积 fg 是这样的映射：$\forall\alpha\in\Omega$，$fg(\alpha)=f(\alpha)g(\alpha)$，试证 Ω^G 是群.

3. 求证：群 G 的全体自同构关于映射的合成运算构成一个群（记为 $\mathrm{Aut}G$）.

4. 求证：若群 G 的每一个元素都适合方程 $x^2=e$，则 G 是 Abel 群.

5. 求证：在一个有限群里阶大于 2 的元素的个数一定是偶数.

6. 假设 G 是一个阶为偶数的有限群. 求证：在 G 里阶等于 2 的元素的个数一定是奇数.

7. 求证：一个有限群的每一个元素的阶都有限.（注：反之未必. 例如，$G=\bigcup_{m=1}^{\infty}\{x\mid x^m=1\}$，即 G 为所有单位根的集合. G 是无限群（按复数的乘法），但 G 中每一个元都是有限阶的.）

8. 设 $f:G\to H$ 是群的同态，g 是 G 的一个有限阶元素，求证：$f(g)$ 的阶整除 g 的阶.

9. 求证：有理数加法群 Q 与非零有理数乘法群 Q^* 不同构.

10. 设 $f(a)=a^{-1}$，$\forall a\in G$. 求证：f 是群 G 的自同构当且仅当 G 是 Abel 群.

11. 假定 τ 是集合 A 的一个非一一变换. 是否存在 τ 的右逆元 τ^{-1}，使得 $\tau\tau^{-1}=id_A$？

12. 求证：一个变换群的单位元一定是恒等变换.

13. 确定 S_5 中元素 $\sigma\tau,\sigma^{-1}\tau\sigma,\sigma^2$，其中 $\sigma=\begin{pmatrix}12345\\23154\end{pmatrix}$，$\tau=\begin{pmatrix}12345\\34152\end{pmatrix}$

14. 列出 S_3 的群表（即乘法运算表）.

15. 将 $\sigma=(456)(567)(761)$ 写成不相交的轮换的乘积.

16. 讨论置换 $\sigma=\begin{pmatrix}1 & 2 & \cdots & n\\ n & n-1 & \cdots & 1\end{pmatrix}$ 的奇偶性.

17. 设 H 是群 G 的非空子集，且 H 的每一个元的阶都有限. 求证：H 构成子群的充要条件是 $\forall a,b\in H$，$ab\in H$.

18. 假定 $\sim$ 是群 G 的元素间的一个等价关系，且对任意的 $a,x,x'\in G$，有 $ax\sim ax'$ 可

推出$x \sim x'$. 求证:与G的单位元e等价的元素作成的集合是G的一个子群.

19. 设G为Abel群,$n \in Z^+$. 试证:$H=\{g \in G | g^n=e\}$是G的子群.

20. 设A,B是群G的两个子群. 求证:$A \cup B$是G的子群当且仅当$A \subseteq B$或$B \subseteq A$. 利用这个事实证明:群G不能被它的两个真子群所覆盖(即表为两个真子群的并).

21. 设A是群G的子群,求证:$\forall g \in G, g^{-1}Ag$也是$G$的子群(称为$A$的共轭子群).

22. 设M是群G的子集,$N_G(M)=\{g \in G | g^{-1}Mg=M\}$,求证:$N_G(M)$是$G$的子群(称为$M$的正规化子).

23. 设A,B是群G的两个子集,若存在$g \in G$,使$g^{-1}Ag=B$,则称A与B共轭. 求证:与A共轭的子集个数等于$[G:N_G(A)]$.

24. 设G为群,对每个元素$g \in G$,定义$f_g:G \to G, f_g(x)=g^{-1}xg, \forall x \in G$. 试证:

(1) f_g是G的自同构;

(2) f_g是恒等自同构当且仅当$g \in C(G)$,其中$C(G)=\{g \in G | \forall a \in G, ag=ga\}$.

25. 设$G=\langle a \rangle, |G|=n$,求证:若$(r,n)=1$,则$G=\langle a^r \rangle$.

26. 设G是循环群,且G与$\overline{G}$同态(即存在从G到$\overline{G}$的满同态),求证:$\overline{G}$也是循环群.

27. 设G是无限阶循环群,$\overline{G}$是任意循环群,证明G与$\overline{G}$同态(即存在从G到$\overline{G}$的满同态).

28. 找出模12的剩余类加群的所有子群.

29. 求证:阶是素数的群一定是循环群.

30. 求证:群G没有非平凡子群的充分必要条件是$G=\{e\}$或G是素数阶循环群.

31. 设a是群G的m阶元素,则a^k为m阶元素的充要条件是$(m,k)=1$.

32. 设G为一个群,$a,b \in G$,a,b的阶分别为m,n,$ab=ba$,$\langle a \rangle \cap \langle b \rangle = \{e\}$. 求证:$ab$的阶为$[m,n]$($[m,n]$为$m,n$的最小公倍数).

33. 写出S_3的全部子群及其左、右陪集,并指出哪些是正规子群.

34. 设群G的正规子群N的阶是2,求证:G的中心包含N.

35. 求证:指数为2的子群一定是正规子群.

36. 设H是G的子群,N是G的正规子群,求证:HN是G的子群.

37. 设M是群G的子群,N是M的子群.

(1) 求证:若$N \lhd G$,则$N \lhd M$;

(2) 若$N \lhd M$,N是否一定是G的正规子群?

38. 设 G 是循环群，N 是 G 的子群，证明：G/N 也是循环群.

39. 设 $N \lhd G$，g 是群 G 的任意一个元素，如果 g 的阶和 $|G/N|$ 互素，求证：$g \in N$.

40. 设 $f: G \to H$ 是群同态，证明：若 g 是 G 的一个有限阶元素，则 $f(g)$ 的阶整除 g 的阶.

41. 设群 G 与群 $\overline{G}$ 同态，$\overline{N}$ 是 $\overline{G}$ 的正规子群，$\overline{N}$ 的原象为 N，求证：$G/N \cong \overline{G}/\overline{N}$.

42. 设 G 和 $\overline{G}$ 分别为 m 阶和 n 阶的循环群，求证：G 与 $\overline{G}$ 同态的充要条件是 $n \mid m$.

第3章　环与域

环是带有两个特殊代数运算的集合，是建立在群上的一个代数系统．环的许多概念与理论是群的相应内容的推广．但由于比群多了一个代数运算，它涵盖的内容要比群丰富，难度也更大．域是一个特殊的环，它包含两个群结构．现在信息及计算机科学中所涉及的运算大部分是域上的．

3.1　环的基本概念及性质

3.1.1　环的定义

首先给出环的定义和几类特殊的环．

定义 3.1.1　如果非空集合 R 带有运算 $+$ 和 $\cdot$（分别称之为加法和乘法），并且满足下列条件：

（1）R 对加法做成交换群；

（2）R 对于乘法是封闭的并且满足结合律；

（3）乘法对加法满足左、右分配律．即对 $\forall a,b,c\in R$ 有

$$a(b+c)=ab+ac,\quad (b+c)a=ba+ca.$$

则称 R 是一个环．

例 3.1.1　（1）全体整数的集合 $\mathbf{Z}$ 对于普通的加法和乘法构成一个环，称为整数环．

（2）全体偶数的集合 $2\mathbf{Z}$ 对于普通的加法和乘法构成一个环．

（3）全体 n 阶实矩阵对于矩阵的加法和乘法构成环．

（4）数域 P 上的一元多项式集合 $P[x]$ 关于多项式的加法和乘法构成环，称为数域 P 上的一元多项式环．

(5) 设 $Z[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in\mathbf{Z},\mathrm{i}=\sqrt{-1}\}$，$Z[\mathrm{i}]$关于复数的加法和乘法构成环，称为 Gauss 整数环.

事实上，我们通常认为整数环、数域 P 上的一元多项式环和数域 P 上的 n 阶矩阵环为环的三大来源.

例 3.1.2　设 $Z_n=\{[0],[1],\cdots,[n-1]\}$是模 n 的剩余类集合，在 Z_n 中已有加法运算$[a]+[b]=[a+b]$，现定义乘法$[a][b]=[ab]$，则这个乘法是 Z_n 上的代数运算，并且 Z_n 关于上述加法和乘法构成一个环，称为模 n 剩余类环.

证明　先证明$[a][b]=[ab]$是代数运算，即说明运算结果与剩余类的代表元选择无关.

若$[a]=[a']$，$[b]=[b']$，即 $n\mid(a-a')$，$n\mid(b-b')$.

由等式

$$ab-a'b'=ab-ab'+ab'-a'b'=a(b-b')+(a-a')b',$$

易知当 $n\mid(a-a')$，$n\mid(b-b')$时，$n\mid ab-a'b'$. 即当

$$[a]=[a'],[b]=[b'],$$

有

$$[ab]=[a'b'].$$

从而证明了上述定义的乘法是 Z_n 上的代数运算.

由群的知识可知，Z_n 关于加法构成交换群. 对乘法来说，封闭性是显然的. 对于任意的元素$[a]$，$[b]$，$[c]\in Z_n$，有

$$([a][b])[c]=[ab][c]=[(ab)c]=[a(bc)]=[a][bc]=[a]([b][c]),$$

即 Z_n 的乘法满足结合律. 又

$$([a]+[b])[c]=[a+b][c]=[(a+b)c]=[ac+bc]=[ac]+[bc]=[a][c]+[b][c],$$

同理$[c]([a]+[b])=[c][a]+[c][b]$，即乘法对加法满足两个分配律.

总之，Z_n 关于上述加法和乘法构成一个环.

从环的定义可以看出，环具有两个独立的二元运算，互相不能代替，但它们不是孤立的，而是通过乘法对于加法的左右分配律紧密联系在一起的. 在环中，这两个运算通过分配律融为一体，由此才形成了具有两个代数运算的环的结构理论.

环本身对加法构成交换群，称之为加群. 为了区分两个运算中的某些特殊元素，我们把加法的单位元称为零元，用 0 表示，元素 a 关于加法的逆元称为 a 的负元，用$-a$ 表示.

3.1.2　几类特殊的环

下面介绍几类特殊的环，它们都是根据环中乘法的特点进行区分的.

定义 3.1.2 若环 R 中的乘法适合交换律，即 $\forall a,b\in R$，有 $ab=ba$，则称 R 为交换环.

若环 R 中有单位元(相对于乘法)，即 $\exists e\in R$，使得 $\forall a\in R$，有 $ae=ea=a$，则称 R 为幺环(或含幺环). 将单位元(也称幺元)记为 1(注：幺环中的幺元是唯一的).

既含幺元又交换的环称为含幺交换环，或交换幺环.

设 a 是含幺环 R 中的元素，如果存在 $b\in R$，使 $ab=ba=1$，则称 b 为 a 的逆元(注：a 若有逆元，则逆元是唯一的)，也称 a 是可逆的.

含幺环 R 中的可逆元称为 R 的单位(或正则元)，容易证明 R 中全体单位对乘法构成群，称为 R 的单位群.

在环中还有一类重要的元素称为"零因子".

定义 3.1.3 若 R 中元素 $a\neq 0,b\neq 0$，但 $ab=0$，则称 a 为 R 的一个左零因子，b 为 R 的一个右零因子. 若一个元素既是左零因子又是右零因子，则称它为零因子.

定义 3.1.4 没有零因子的环称为无零因子环，由此可知，R 是无零因子环$\Leftrightarrow\forall a,b\in R$，当 $ab=0$ 时，有 $a=0$ 或 $b=0$.

无零因子的交换幺环称为整环.

例如，在二阶实方阵关于矩阵的加法和乘法构成的环中，零元就是零矩阵 0. 矩阵

$$\boldsymbol{A}=\begin{pmatrix}1&0\\0&0\end{pmatrix}\neq 0,\boldsymbol{B}=\begin{pmatrix}0&0\\1&0\end{pmatrix}\neq 0,\boldsymbol{C}=\begin{pmatrix}0&1\\0&0\end{pmatrix}\neq 0.$$

但是 $\boldsymbol{AB}=0$，所以矩阵 $\boldsymbol{A}$ 是左零因子，矩阵 $\boldsymbol{B}$ 是右零因子. 又 $\boldsymbol{CA}=0$，所以矩阵 $\boldsymbol{A}$ 是环的一个零因子.

当然，在交换环中，所有的左零因子都是右零因子，从而就是零因子了. 例如，在模 6 剩余类环 Z_6 中，[2]和[3]都是零因子.

容易验证，整数环是一个无零因子环，而且整数的乘法满足交换律，1 是单位元，所以整数环是一个整环. 同样数域 P 上的一元多项式环也是整环.

零因子判断还有没有其它的方法？它与环的性质之间有怎样的关系？我们将在这一节的后半部分介绍. 下面我们先介绍另外两类重要的环——除环和域.

定义 3.1.5 一个环 R 称为除环(体)，如果

(1) R 中至少包含一个不等于零的元；

(2) R 有单位元；

(3) R 的每一个不等于零的元有逆元.

定义 3.1.5′ 若环 R 中的非零元全体对于乘法构成群，则称 R 为一个除环. 此时 R

中全体非零元构成的乘法群称为 R 的乘群，记为 $R^* = R\backslash\{0\}$.

定义 3.1.6　若 R 是交换的除环，则称 R 为域.

例 3.1.3　设 $H=\left\{\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\middle|\alpha,\beta \text{ 为复数}\right\}$为二阶复方阵的集合，

(1) 易见 H 关于矩阵的加法构成 Abel 群，零元为 $\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.

(2) $\forall \alpha,\beta,\gamma,\delta\in C$(复数集合)

$$\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\begin{pmatrix}\gamma & \delta\\ -\bar{\delta} & \bar{\gamma}\end{pmatrix}=\begin{pmatrix}\alpha\gamma-\beta\bar{\delta} & \alpha\delta+\beta\bar{\gamma}\\ -\bar{\beta}\gamma-\bar{\alpha}\bar{\delta} & -\bar{\beta}\delta+\bar{\alpha}\bar{\gamma}\end{pmatrix}\in H,$$

即 H 对乘法封闭，矩阵乘法适合结合律.

(3) 矩阵的加法与乘法适合左，右分配律，因此 H 对于矩阵的加法与乘法构成环.

任取 H 中非零元 $\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}\neq\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$，则 $\begin{vmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{vmatrix}=|\alpha|^2+|\beta|^2>0$,

即非零元有逆元.

$$\begin{pmatrix}\alpha & \beta\\ -\bar{\beta} & \bar{\alpha}\end{pmatrix}^{1}=\frac{1}{|\alpha|^2+|\beta|^2}\begin{pmatrix}\bar{\alpha} & -\beta\\ \bar{\beta} & \alpha\end{pmatrix}\in H.$$

因此 H 是一个体. 另外 H 中元素 $\boldsymbol{A}=\begin{pmatrix}i & 0\\ 0 & -i\end{pmatrix}$，$\boldsymbol{B}=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$，有 $\boldsymbol{AB}\neq\boldsymbol{BA}$，故 H 是非交换的体，称 H 为四元数体.

例 3.1.4　有理数全体 **Q** 对数的加法和乘法构成域；实数全体 **R** 对数的加法和乘法构成域.

例 3.1.5　当 $n=p$ 为素数时，模 n 剩余类环 Z_n 是域.

证明　显然环 Z_n 的乘法满足交换律，所以只需再证 $Z_p\backslash\{0\}$是一个乘群即可.

因为乘法适合结合律，又 $Z_p\backslash\{0\}$是一个有限集合，由群的等价定义(详见定义 2.1.4)，只需再证明封闭性和消去律成立.

(1) 封闭性

由于 p 是素数，$p\nmid a$，$p\nmid b\Rightarrow p\nmid ab$，即若$[a]\neq 0$，$[b]\neq 0\Rightarrow[a][b]\neq 0$. 换言之，$[a]$，$[b]\in Z_p\backslash[0]\Rightarrow[a][b]=[ab]\in Z_p\backslash[0]$

(2) 消去律

若

$$\left.\begin{array}{c} p \mid ax-ax'=a(x-x') \\ p \nmid a \end{array}\right\} \Rightarrow p \mid (x-x'),$$

即若$[ax]=[ax'],[a]\neq[0]\Rightarrow[x]=[x']$.

换言之,$[a][x]=[a][x'],[a]\in Z_p\backslash[0]\Rightarrow[x]=[x']$.

综上,Z_p 是域.

具有有限个元素的域,称为有限域.为了纪念近世代数的开创人 Galois,有限域也称 Galois 域.Z_p(p 是素数)是最简单的有限域.

3.1.3 环的简单性质

设 R 是一个环,先做如下约定:

$$ma=\overbrace{a+a+\cdots+a}^{m},m\in Z^+,$$

$$-ma=\overbrace{(-a)+(-a)+\cdots+(-a)}^{m},$$

$$a^0=1(\text{若环 } R \text{ 中有幺元}).$$

则 R 有如下性质:

性质 3.1.1 $(m+n)a=ma+na,\forall a\in R,m,n\in Z$;

$(mn)a=m(na),\forall a\in R,m,n\in Z$;

$m(a+b)=ma+mb,\forall a,b\in R,m\in Z$;

$a^m a^n=a^{m+n},(a^m)^n=a^{mn},\forall a\in R,m,n\in Z^+$.

若 a 有逆元,则 $a^m a^n=a^{m+n}$, $(a^m)^n=a^{mn},\forall a\in R,m,n\in Z$.

性质 3.1.2 $\left(\sum\limits_{i=1}^{n}a_i\right)\left(\sum\limits_{j=1}^{m}b_j\right)=\sum\limits_{i=1}^{n}\sum\limits_{j=1}^{m}a_ib_j,\forall a_i,b_j\in R$.

性质 3.1.3 $\forall a,b\in R$,有 $a\cdot 0=0\cdot a=0;(-a)b=a(-b)=-ab;(-a)(-b)=ab$.

证明 因为 $a\cdot(0+0)=a\cdot 0+a\cdot 0=a\cdot 0$,故 $a\cdot 0=0$.类似可证 $0\cdot a=0$.

$(-a)b+ab=[(-a)+a]b=0\cdot b=0$,故$(-a)b=-ab$.类似可证明 $a(-b)=-ab$, $(-a)(-b)=-[a(-b)]=-[-ab]=ab$.

3.1.4 无零因子环的性质与特征

定理 3.1.1 若环 R 是无零因子环,则 R 中两个消去律都成立.即如果 $a\neq 0,ab=ac$,则$b=c$,且如果 $a\neq 0,ba=ca$,则 $b=c$.

证明 因为 R 无零因子，$a\neq 0, ab=ac\Rightarrow(ab-ac)=0\Rightarrow b=c$. 同理 $a\neq 0, ba=ca\Rightarrow b=c$.

定理 3.1.2 若环 R 中成立一个消去律，则 R 无零因子.

证明 （反证法）如果 R 有零因子，即存在 $a\neq 0, b\neq 0, ab=0$，设环 R 中成立左消去律，即 $\forall a,b,c\in R, a\neq 0$，由 $ab=ac\Rightarrow b=c$. 在此消去律下

$$ab=0\Rightarrow a\cdot b=a\cdot 0=0\Rightarrow b=0,$$

与 $b\neq 0$ 矛盾.

由定理 3.1.1 和定理 3.1.2 不难得到下面结论.

推论 3.1.1 若环 R 中成立一个消去律，则另一个消去律也成立.

推论 3.1.2 环 R 无零因子的充要条件是 R 中成立两个消去律.

接下来我们研究无零因子环中，元素关于加法的阶的性质.

设 R 是一个环，$a\in R, a\neq 0$，若 a 在加法群中的阶为 n，则

$$\underbrace{a+a+\cdots+a}_{n}=na=0.$$

若 a 在加法群中的阶为无限大，则 $\forall n\in Z, na\neq 0$.

因此，在一般环中，由 $a\neq 0$ 能否得到 $\forall k\in Z, ka\neq 0$，取决于 a 在加法群中的阶是否有限. 有的非零元在加法群中的阶是有限的，有的阶却是无限的. 不过，对于无零因子环而言情况就有些特殊了.

定理 3.1.3 设 R 为无零因子环，则 R 中非零元对加法来说阶是相同的.

证明 任取元素 $a,b\in R, a\neq 0, b\neq 0$.

若 a 的阶（对加法而言）为有限数 n，则 $na=0, (na)b=a(nb)=0$. 因为 R 中无零因子，故 $nb=0$. 因此 b 也是有限阶的，且 b 的阶 $\leqslant a$ 的阶. 由 a,b 的任意性可知 a 的阶 $\leqslant b$ 的阶，故 a 与 b 的阶相同.

若 a 为无限阶的元素，则 b 也为无限阶元素，否则由上面的证明可知 a 与 b 同为有限阶元素.

可见，无零子环中所有非零元关于加法的阶，是环的一个代数性质，称之为特征.

定义 3.1.7 设 R 为环，如果存在正整数 m，使得 $\forall r\in R$，均有 $mr=0$，则将满足此条件的最小正整数 m 称为环 R 的特征，记为 $\mathrm{char}R$.

若不存在这样的正整数 m，则称环 R 的特征是零.

$\mathrm{char}R=1$ 当且仅当 $R=\{0\}$ 为零环.

定理 3.1.4 无零因子环 R 的特征若为正整数 n，则 n 为素数.

证明 若 n 不是素数，设 $n=n_1n_2$，且 $1<n_1, n_2<n$.

$\forall a\neq 0, a\in R$，可知 a 在加法群中的阶为 n，故 $n_1a\neq 0, n_2a\neq 0$，但

$$(n_1a)(n_2a)=(n_1n_2)aa\neq 0=(na)a=0,$$

与 R 是无零因子环矛盾.

推论 3.1.3 整环、除环与域的特征或者是零，或者是素数 p.

在一个特征是 p 的交换环里，

$$(a+b)^p=a^p+C_p^1a^{p-1}b+\cdots+C_p^{p-1}ab^{p-1}+b^p,$$

而 C_p^i 是 P 的倍数，故 $C_p^ia^{p-i}b^i=0$.

所以

$$(a+b)^p=a^p+b^p.$$

这个等式称为环中的二项式定理.

3.2 子环和理想子环

这一节我们讨论环的具有某些性质的子集.

3.2.1 子环

定义 3.2.1 环 R 的非零子集 S 若对于环 R 中的运算(加法和乘法)也构成环，则称 S 为 R 的子环，R 也称为 S 的扩环.

类似可以定义子除环、子域的概念.

从环的定义不难看出，S 是 R 的子环，当且仅当 S 对于加法来说是 R 的子群，且对于乘法封闭. 我们将其总结为以下定理.

定理 3.2.1 设 S 是环 R 的非空子集，则 S 构成子环的充要条件是

$$\forall a,b\in S, a-b\in S, ab\in S.$$

类似地我们很容易得到：

定理 3.2.2 设 S 是除环(域)R 的非空子集，则 S 构成子除环(子域)的充要条件是

$$\forall a,b\in S, a-b\in S, ab^{-1}\in S(b\neq 0).$$

例 3.2.1 $2\mathbf{Z}$(偶数集)是 $\mathbf{Z}$ 的子环，$\mathbf{Z}$ 是 $\mathbf{Q}$ 的子环.

例 3.2.2 若 S 是 $\mathbf{Z}$ 的非空子环，则 S 是 $\mathbf{Z}$ 的加法子群，而 $\mathbf{Z}$ 是加法循环群，因此 S 也是加法循环群，即存在 $n\in N$，使 $S=n\mathbf{Z}$. 显然每个 $n\mathbf{Z}$ 都是 $\mathbf{Z}$ 的子环，因此 $\mathbf{Z}$ 的全部子环为 $n\mathbf{Z}, n\geqslant 0$.

值得注意的是，环和子环在单位元方面没有必然关系，这和群与子群的关系不一样. 设 S 是环 R 的子环，当 R 有单位元时，S 不一定有；当 S 有单位元时，R 不一定有；即使二者都有单位元，此二者也未必相同. 请大家用整数环、偶数环和零环来验证.

3.2.2　理想子环

下面我们讨论一个特殊的子环，它在环中的作用如同正规子群在群中的作用.

我们先在环 R 的加群中来构造商群.

设 S 是环 R 的子环，则 S 是交换群 R 的子群，于是有加法商群 R/S，R/S 中已有加法 $[a]+[b]=[a+b]$，我们希望在 R/S 上自然地定义乘法 $[a][b]=[ab]$，使得 R/S 是环. 为此，需要对 S 加些限制，由此引入理想的概念.

定义 3.2.2　环 R 的子环 I 称为 R 的理想子环，简称理想，如果 $\forall a\in I, r\in R$，有

$$ar, ra\in I.$$

从集合的角度来定义理想，它的等价定义为环 R 的非空子集 I 称为 R 的理想，如果

$$\begin{cases}\forall a,b\in I & a-b\in I \\ \forall r\in R & ar\in I, ra\in I\end{cases},$$

显然 $\{0\}$ 和 R 本身是环 R 的理想，称它们为 R 的平凡理想.

例 3.2.1　$n\mathbf{Z}$ 是 $\mathbf{Z}$ 的理想($n\in Z$).

例 3.2.2　写出 Z_6 的所有理想.

解　首先写出 Z_6 的子加群，然后从中选出满足理想乘法性质的子集，即为理想.

$I_1=\{[0]\}$,

$I_2=\{[0],[3]\}$,

$I_3=\{[0],[2],[4]\}$,

$I_4=Z_6$.

关于理想的定义，需要注意以下几点：

(1) 环 R 的理想 I 是加群 R 的子加群，反之不对.

例如，Z 是 Q 的子加群，但整数环不是 Q 的理想.

(2) 理想是子环，反之不对.

例如，$\left\{\left.\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}\right| a,b,c\in Z\right\}$是 2 阶矩阵环的子环，但不是理想，可见理想对乘法具有更强的封闭性.

(3) 理想不具有传递性,即环的理想的理想不一定是原环的理想.

例如,令 F 是一个域,如下取 F 上的三类矩阵的集合:

$$I=\left\{\begin{pmatrix}0&0&0\\0&0&a\\0&0&0\end{pmatrix}\middle| a\in F\right\},\quad N=\left\{\begin{pmatrix}0&0&x\\0&0&y\\0&0&0\end{pmatrix}\middle| x,y\in F\right\},$$

$$R=\left\{\begin{pmatrix}a_1&a_2&a_3\\0&a_4&a_5\\0&0&a_6\end{pmatrix}\middle| a_i\in F,i=1,2,\cdots,6\right\}.$$

可见 I 是 N 的理想,N 是 R 的理想,但 I 不是 R 的理想.

定义 3.2.3 只有平凡理想的环称为单环.

例 3.2.3 除环 R 是单环.

证明 设 I 是除环 R 的任意理想,如果 $I\neq\{0\}$,在 I 中取非零元 a,则 a 有逆元 $a^{-1}\in R$. 又 I 为理想,故

$$a^{-1}a=1\in I.$$

对 R 中任意元素 b,有

$$b1=b\in I,$$

即 $I=R$. 这说明除环 R 只有平凡理想,所以除环 R 是单环.

由此可以看出,理想对除和域没有太大意义.

3.2.3 主理想、极大理想和素理想

在这一部分介绍几个重要理想:主理想、极大理想和素理想.

定义 3.2.4 设 R 为环,$a\in R$,$a\neq 0$,I 为包含元素 a 的一个理想. 如果对于任意包含 a 的理想 U,都有 $I\subseteq U$,也就是说 I 是 R 中包含 a 的最小理想,称 I 为由 a 生成的主理想,记为 (a).

例如,在整数环 Z 中,$2Z$ 和 $3Z$ 分别是由 2 和 3 生成的主理想.

接下来我们考察一下主理想 (a) 的结构,看看主理想 (a) 是有哪些元素构成的.

首先,由于 $a\in(a)$,所以对任意整数 n,有

$$na\in(a);$$

其次,对于 R 中任意元素 r_1,r_2 及 $x_i,y_i(i=1,2,\cdots,n)$ 有

$$r_1a,\quad ar_2,\quad x_iay_i\in(a);$$

从而 (a) 包含所有这些元素的和,即

$$x_1ay_1+x_2ay_2+\cdots+x_may_m+r_1a+ar_2+na.$$

另外，上述所有这种形式的元素集合做成一个包含元素 a 的理想，因此

$$(a)=\{x_1ay_1+x_2ay_2+\cdots+x_may_m+r_1a+ar_2+na \mid x_i, y_i, r_i\in R, n\in Z, m\geqslant 1\}.$$

令

$$Za=\{na \mid n\in Z\}, Ra=\{ra \mid r\in R\}, aR=\{ar \mid r\in R\},$$

$$RaR=\{x_1ay_1+x_2ay_2+\cdots+x_may_m \mid x_i, y_i\in R, 1\leqslant i\leqslant m\}$$

由 a 生成的主理想记为

$$(a)=Za+Ra+aR+RaR.$$

主理想的表达形式看起来比较复杂，但当环 R 具有某些性质时，它的形式可以进行化简.

(1) R 是交换环时，$(a)=Za+Ra$. 这是因为

$$\begin{aligned}&x_1ay_1+x_2ay_2+\cdots+x_may_m+r_1a+ar_2\\&=(x_1y_1+x_2y_2+\cdots+x_my_m+r_1+r_2)a\\&=ra\in Ra.\end{aligned}$$

(2) R 是含幺环时，$(a)=RaR$. 这是因为

$$r_1a+ar_2+na=r_1a\cdot 1+ar_2\cdot 1+(n\cdot 1)a\cdot 1\in RaR.$$

(3) R 是含幺交换环时，$(a)=Ra=aR$.

下面进一步推广主理想的概念.

定义 3.2.5 设 X 是环 R 的子集，包含 X 的最小理想称为由 X 生成的理想，记为 (X).

类似主理想的讨论，我们得到 (X) 的结构.

设 $X=\{s_1, s_2, \cdots, s_t\}$，则

$$(X)=ZX+XR+RX+RXR=(s_1)+(s_2)+\cdots+(s_t),$$

其中，

$$ZX=\left\{\sum_{i=1}^{n}k_is_i \mid s_i\in X, k_i\in Z, n\geqslant 1\right\},$$

$$RX=\left\{\sum_{i=1}^{t}r_is_i \mid s_i\in X, r_i\in R, t\geqslant 1\right\},$$

$$XR=\left\{\sum_{i=1}^{t}s_ir_i \mid s_i\in X, r_i\in R, t\geqslant 1\right\},$$

$$RXR=\left\{\sum_{i=1}^{t}r_is_i\tilde{r_i} \mid s_i\in X, r_i, \tilde{r}_i\in R, t\geqslant 1\right\}.$$

特别地，R 是含幺交换环时，$(X)=XR=s_1R+s_2R+\cdots+s_tR$.

应当注意，由多个元素生成的理想，也可能是个主理想，即也可能由一个元素生成.

例 3.2.4 设 R 为整数环，求证 $(3,7)=(1)$

证明 $1\in(1)\Rightarrow 1+1+1=3\in(1)$，$7=\overbrace{1+1+\cdots+1}^{7}\in(1)\Rightarrow(3,7)\subseteq(1)$. 反之，$(3)\in(3,7)$，$(7)\in(3,7)\Rightarrow -3\in(3,7)$，$1=(-3)+(-3)+7\in(3,7)$. 故 $(1)\subseteq(3,7)$，所以 $(3,7)=(1)$.

将这个例子推广到一般情形，若整数 $a_1,a_2,\cdots,a_m$ 的最大公因子是 d，则

$$(a_1,a_2,\cdots,a_m)=(d).$$

另外也容易证得，若 I 是整数环 Z 的一个非零理想，a 是 I 中最小正整数，则

$$I=(a).$$

由此可见，整数环的所有理想都是主理想.

定义 3.2.6 设 R 是一个交换环，P 是 R 的一个理想，如果 $\forall a,b\in R$，当 $ab\in P$ 时，有 $a\in P$ 或 $b\in P$，称 P 是 R 的素理想.

例 3.2.5 整数环 Z 的全部素理想是：$\{0\}$，Z 以及由所有素数 p 生成的理想 (p).

证明 这些理想显然都是 Z 的素理想. 又由于整数环 Z 的理想都是主理想，因此，如果 n 是一个合数，设

$$n=n_1n_2,\quad 1<n_1,n_2<n,$$

则有 $n_1n_2=n\in(n)$，但是 $n\nmid n_1$，$n\nmid n_2$，即有

$$n_1\notin(n),\quad n_2\notin(n),$$

即 (n) 不是整数环 Z 的素理想.

例 3.2.6 设 p 为素数，$(2p)$ 是偶数环 $2Z$ 的主理想，试问 $(2p)$ 是素理想吗？

解 当 $p=2$ 时，(4) 不是素理想. 因为

$$2\cdot 2=4\in(4),\quad 但\ 2\notin(4).$$

当 p 为奇素数时，$(2p)$ 是素理想.

事实上，设 $ab\in(2p)$，其中 a,b 都是偶数. 又设

$$a=2s,b=2t,ab=2(2st)=2pq,$$

其中 s,t,q 为整数. 由于 p 为奇素数，故可知 $p\mid st$. 从而

$$p\mid s\ 或\ p\mid t.$$

由此可知 $a\in(2p)$ 或 $b\in(2p)$，即 $(2p)$ 是偶数环的素理想.

定义 3.2.7 环 R 中的理想 M 称为 R 的极大理想，须满足：

(1) $M\neq R$；

(2) 对于 R 的任意理想 N，若 $M\subseteq N\subseteq R$，则 $N=M$ 或 $N=R$.

例 3.2.7　设 p 是素数，则(p)是整数环 Z 的极大理想，进一步，它们是整数环的所有极大理想.

证明　设 p 是素数，I 是整数环 Z 的一个理想，且

$$(p)\subset I\subseteq Z.$$

则取 $k\in I$，$(k,p)=1$，故存在 $m,n\in Z$，使

$$1=mk+np\in I,$$

即 $I=Z$，所以(p)是整数环 Z 的极大理想.

再者，设 M 是 Z 的极大理想，由于 Z 的理想都是主理想，故可设 $M=(m)$，且不妨设 m 是正整数. 如果 m 是合数，令

$$m=m_1m_2,1<m_1,m_2<m.$$

则由 m_1 生成的理想$(m_1)\neq Z$，$(m_1)\neq M$，但却有

$$M=(m)\subset(m_1),$$

这与 M 是 Z 的极大理想矛盾，故 m 是素数.

从例 3.2.4 和例 3.2.6 可以看出，除平凡理想外，整数环的素理想和极大理想是一致的. 但对其他环来说并不是这样. 读者可以举些例子，特别是在多项式环中可以找到这样的例子.

3.3　环的同态与商环

为了比较不同的环，我们引入环的同态、同构及环同态基本定理，进一步讨论商环与极大理想及素理想之间的关系.

3.3.1　环的同态

定义 3.3.1　设 R 和 S 为环，$f:R\to S$ 为环 R 到 S 的映射. 如果 $\forall a,b\in R$，有

$$f(a+b)=f(a)+f(b),$$
$$f(ab)=f(a)f(b).$$

则称 f 为 R 到 S 的同态映射.

当 f 为单射时称为单同态映射；

当 f 为满射时称为满同态映射，此时称环 R 和 S 同态；

f 为一一映射时称为同构映射,此时称环 R 和 S 同构,记为 $R\cong S$;

特别地,当 $R=S$ 时,称 f 为自同构映射.

定义环 R 到环 S 的映射 f 为

$$f(r)=0_S,\quad \forall r\in R.$$

其中 0_S 为环 S 的零元. 显然 f 是环 R 到环 S 的同态映射. 我们称此同态映射为零同态.

由此可以看出任意两个环之间都存在环同态映射.

例 3.3.1 设 n 为一个整数,定义整数环 Z 到模 n 剩余类环 Z_n 的映射 f 为

$$f(m)=[m],\forall m\in Z$$

因为 $\forall s,t\in Z$,

$$f(s+t)=[s+t]=[s]+[t]=f(s)+f(t),$$

$$f(st)=[st]=[s][t]=f(s)f(t).$$

所以 f 是整数环 Z 到模 n 剩余类环 Z_n 的同态映射. 显然 f 是满射,所以整数环 Z 与模 n 剩余类环 Z_n 同态.

由环同态的定义,可以看出若环 R 和环 S 同态,当然 R 的加群与 S 的加群也同态. 为此,我们可以把群同态的一些性质直接推广到环中.

定理 3.3.1 设 $f:R\to\overline{R}$ 是环 R 到 $\overline{R}$ 的满同态映射,则

(1) $f(0_R)=\overline{0}_{\overline{R}}, f(-a)=-f(a)$;

(2) 若 R 是交换环,则 $\overline{R}$ 亦为交换环;

(3) 若 R 是含幺环,则 $\overline{R}$ 亦为含幺环,且 $f(1_R)=\overline{1}_{\overline{R}}$.

其中 $0_R,\overline{0}_{\overline{R}},1_R,\overline{1}_{\overline{R}}$ 分别是 R 和 $\overline{R}$ 的零元和单位元.

证明 (1) 由群同态性质,直接可以推得前两个等式.

(2) 设 R 是交换环. $\forall \overline{a},\overline{b}\in\overline{R}$,因为 f 是满射,可令

$$f(a)=\overline{a},f(b)=\overline{b},$$

其中 $a,b\in R$.

而

$$\overline{a}\,\overline{b}=f(a)f(b)=f(ab)=f(ba)=f(b)f(a)=\overline{b}\,\overline{a},$$

所以 $\overline{R}$ 也是交换环.

(3) 设 R 是含幺环,

$$\overline{a}f(1_R)=f(a)f(1_R)=f(a1_R)=f(a)=\overline{a},$$

所以 $f(1_R)=\overline{1}_{\overline{R}}$ 是 $\overline{R}$ 的单位元,即 $\overline{R}$ 也是含幺环.

定理 3.3.2 设 $f:R\to\overline{R}$ 是环 R 到 $\overline{R}$ 的满同态映射,则

(1) R 的子环 S 的象 $\overline{S}$ 是 $\overline{R}$ 的子环；

(2) R 的理想 I 的象 $\overline{I}$ 是 $\overline{R}$ 的理想；

(3) $\overline{R}$ 的子环 $\overline{S}$ 的原象是 R 的子环 S；

(4) $\overline{R}$ 的理想 $\overline{I}$ 的原象是 R 的理想 I.

证明　(1) 因为 f 为满射，所以对于任意的元素 $\overline{s}_1,\overline{s}_2\in\overline{S}$ 在 S 中存在原象，令

$$f(s_1)=\overline{s}_1,\ f(s_2)=\overline{s}_2,$$

其中 $s_1,s_2\in S$.

因为 S 为子环，所以

$$s_1-s_2\in S, s_1s_2\in S.$$

又 f 为同态映射，从而

$$\overline{s}_1-\overline{s}_2=f(s_1)-f(s_2)=f(s_1-s_2)\in\overline{S},$$

$$\overline{s}_1\ \overline{s}_2=f(s_1)f(s_2)=f(s_1s_2)\in\overline{S}.$$

故 $\overline{S}$ 是 $\overline{R}$ 的子环.

(2)、(3)、(4)可类似证明，在此不再赘述.

从上面两个定理可以看出，同态满射保持了两个环的一些性质是不变的，但同态映射不保持零因子性质. 也就是一个无零因子环可能和有零因子环同态，相反，一个有零因子环也可能和无零因子环同态. 但当两个环同构时，它们的代数性质没有区别.

例 3.3.2　(1) 在例 3.3.1 中取 $n=6$，而 Z_6 是个有零因子环，整数环是无零因子环，这说明一个无零因子环与一个有零因子环同态.

(2) 设 $R=\{(a,b)\mid a,b\in Z\}$，在 R 中定义运算如下：

$$(a_1,b_1)+(a_2,b_2)=(a_1+a_2,b_1+b_2),$$

$$(a_1,b_1)(a_2,b_2)=(a_1a_2,b_1b_2).$$

容易验证 R 关于上述运算做成环，而且(0,0)是其零元.

定义环 R 到整数环的映射如下：

$$\varphi:(a,b)\rightarrow a$$

则 φ 为 R 到 Z 的同态满射. 这说明有零因子环 R 和无零因子环 Z 是同态的.

3.3.2　商环与环同态基本定理

在群论中，由正规子群可以产生商群，并由此得到群论中一些重要结论. 同样，利用理想也可以产生一些新的环，即商环，进一步，可以得到一系列相应的重要结果.

设 I 是环 R 的理想，则 I 是 R 的一个子加群. 对于环 R 的加法来说，I 是 R 的正规子

群.从而 I 的所有陪集

$$[a]=a+I,\quad a\in R$$

构成的集合 R/I,对于陪集的加法

$$[a]+[b]=(a+I)+(b+I)=(a+b)+I=[a+b]$$

构成一个群,即商群.

下面我们在 R/I 上再规定以下乘法：

$$[a][b]=(a+I)(b+I)=(ab)+I=[ab].$$

首先证明这是一个代数运算,即其结果与陪集的代表元的选择无关.

事实上,若$[a]=[a']$,$[b]=[b']$,则有

$$a-a'\in I,b-b'\in I,$$

因为 I 是理想,所以

$$(a-a')b\in I,a'(b-b')\in I.$$

从而

$$(a-a')b+a'(b-b')=ab-a'b'\in I.$$

所以

$$[a][b]=[a'][b'].$$

这说明此运算与代表元的选择无关.

我们把这个代数运算称为陪集的乘法.

容易验证 R/I 关于陪集的加法和乘法构成环,称为商环,也称模 I 的剩余类环.

定理 3.3.3 设 I 是环 R 的理想,映射 $f:R\to R/I,f(r)=[r]$,则 f 为满同态映射.称此映射为环 R 到商环 R/I 的自然同态,一般记为 $\Pi(r)=[r]$.

直接用同态映射的定义就可以验证定理的正确性,请读者自行完成.

类似于群同态基本定理,在环中也有环同态基本定理.

定理 3.3.4 设 f 为环 R 到环 $\overline{R}$ 的满同态映射,则

$$I=\{r\in R\mid f(r)=\overline{0}\}$$

是 R 的理想,称为 f 的核,记为 $\mathrm{Ker}(f)$,其中 $\overline{0}$ 表示环 $\overline{R}$ 的零元;进一步,$R/I\cong\overline{R}$.

证明 (1) 先证明 $\mathrm{Ker}(f)$是 R 的理想.

因为 $f(0)=\overline{0}$,故 $\mathrm{Ker}(f)$是非空集合.

$\forall a,b\in\mathrm{Ker}(f),f(a)=\overline{0},f(b)=\overline{0}$, 故 $f(-b)=-f(b)=\overline{0}$.从而

$$f(a-b)=f(a)+f(-b)=\overline{0}+\overline{0}=\overline{0},$$

即 $a-b\in\mathrm{Ker}(f)$.

$\forall a\in \mathrm{Ker}(f), r\in R$,

$$f(ar)=f(a)f(r)=\bar{0}f(r)=\bar{0},$$
$$f(ra)=f(r)f(a)=\bar{0}.$$

故 $ra, ar\in \mathrm{Ker}(f)$，从而 $\mathrm{Ker}(f)$是 R 的理想.

(2) 再证明 $R/I\cong\overline{R}$.

定义 $\varphi: R/I\to\overline{R}$ 为

$$\varphi([a])=\bar{a}=f(a).$$

先证明 φ 是 R/I 到 $\overline{R}$ 的映射，即陪集的象与代表元的选择无关.

事实上，若$[a]=[b]$，则 $a-b\in \mathrm{Ker}(f)$，于是 $f(a-b)=\bar{0}$，从而 $f(a)=f(b)$，因此 φ 是 R/I 到 $\overline{R}$ 的映射.

又若 $\varphi([a])=\varphi([b])$，并注意到 f 为环 R 到环 $\overline{R}$ 的同态映射，则有

$$f(a)=f(b)\Rightarrow f(a)-f(b)=0\Rightarrow f(a-b)=0,$$

所以 $a-b\in Ker(f)$，故$[a]=[b]$，从而 φ 为单射.

再者，$\forall \bar{r}\in\overline{R}$，因为 f 为 R 到 $\overline{R}$ 的满射，所以 $\exists r\in R$，使得

$$f(r)=\bar{r}.$$

这样就有

$$\varphi([r])=\bar{r}.$$

所以 φ 为满射.

最后，

$$\varphi([a]+[b])=\varphi([a+b])=f(a+b)=\varphi([a])+\varphi([b]),$$
$$\varphi([a][b])=\varphi([ab])=f(ab)=\varphi([a])\varphi([b]).$$

综上所述，φ 为同构映射，即 $R/I\cong\overline{R}$.

定理 3.3.3 说明了任何一个环到它的每一个商环 R/I 都存在着自然同态 Π，也说明环 R 与它的任意商环同态. 定理 3.3.4 说明环 R 的任意同态象必同构于它的某个商环. 从同构的意义上，我们可以说环 R 与且只与它的商环同态.

3.3.3　极大理想、素理想与其商环的关系

利用极大理想可以得到一个域. 为了达到此目的，首先利用极大理想来构造一个单环，即只有平凡理想的环.

定理 3.3.5　设 I 是环 R 的一个理想，则

商环 R/I 是单环$\Leftrightarrow I$ 是环 R 的极大理想.

证明 考虑自然同态 $\Pi: R \to R/I$（Π 的核为 I）. 由定理 3.3.2 可知，R/I 的任意理想 $\overline{B}$ 的原象 B 是 R 的理想.

充分性. 设商环 R/I 是单环，B 是 R 的一个理想，并且

$$I \subseteq B \subseteq R.$$

由定理 3.3.2 可知，$\Pi(B)=\overline{B}$ 是 R/I 的理想.

因为 R/I 是单环，所以

$$\overline{B}=\overline{0} \text{ 或 } \overline{B}=R/I.$$

若 $\overline{B}=\overline{0}$，则 $B=I$；

若 $\overline{B}=R/I$，则 $B=R$.

可见，包含 I 的任意理想 B 只能是 I 或者环 R，所以 I 是环 R 的极大理想.

必要性. 设 I 是环 R 的极大理想. 任意取 R/I 的理想 $\overline{B}$，则由定理 3.3.2 可知，$\overline{B}$ 在 Π 下的原象 B 是 R 的理想，且

$$I \subseteq B \subseteq R.$$

因为 I 是环 R 的极大理想，所以 $B=I$ 或 $B=R$. 当 $B=I$ 时，$\overline{B}=\overline{0}$. 当 $B=R$ 时，$\overline{B}=R/I$. 这说明 R/I 的理想或是零理想或者是环 R/I 本身，也就是说 R/I 是单环.

引理 3.3.1 含幺交换的单环是域.

证明 设 $\tilde{R}$ 是含幺交换的单环. $\forall a \in \tilde{R}, a \neq 0$，$(a)$ 是 $\tilde{R}$ 的非零理想. 因为 $\tilde{R}$ 是单环，所以

$$(a)=\tilde{R}.$$

从而

$$1 \in \tilde{R}=(a).$$

于是存在 $r \in \tilde{R}$，使得

$$ar=ra=1,$$

即 $r=a^{-1}$（注意 $\tilde{R}$ 为含幺交换环，$(a)=a\tilde{R}=\tilde{R}a$），这说明 $\tilde{R}$ 中非零元均有逆，因此 $\tilde{R}$ 为除环，且 $\tilde{R}$ 交换，从而为域.

定理 3.3.6 设 R 是含幺交换环，I 是 R 的理想，则

$$R/I \text{ 是域} \Leftrightarrow I \text{ 是环 } R \text{ 的极大理想}.$$

证明 充分性. 设 R/I 是域，所以 R/I 是单环，由定理 3.3.5 可知 I 是极大理想.

必要性. 设 I 是 R 的极大理想，由定理 3.3.5 可知，R/I 是单环.

易知自然同态是 R 到 R/I 的同态满射，所以 R 与其商环 R/I 同态. R/I 也就是 R 在

自然同态的象. 而 R 是含幺交换环，由定理 3.3.1 可知，R/I 亦为含幺交换环.

总之，R/I 是含幺交换的单环，再由引理 3.3.1，证得 R/I 是域.

类似于极大理想与商环的关系，下面讨论素理想和其商环的关系.

定理 3.3.7　设 R 为含幺交换环，I 为 R 的理想，则

$$R/I \text{ 是整环} \Leftrightarrow I \text{ 是环 } R \text{ 的素理想}.$$

证明　充分性. 设 R/I 是整环，对于任意的元素 $a,b\in R$，如果有

$$ab\in I,$$

则有

$$[ab]=[a][b]=[0].$$

而 R/I 是整环，即 R/I 没有零因子，所以

$$[a]=[0] \text{ 或 } [b]=[0].$$

当 $[a]=[0]$ 时，有 $a\in I$；当 $[b]=[0]$ 时，有 $b\in I$.

也就是

$$\text{如果 } ab\in I, \text{则 } a\in I \text{ 或 } b\in I.$$

从而 I 是环 R 的素理想.

必要性. 因为 R 为含幺交换环，由定理 3.3.1 和定理 3.3.5 可知，R/I 也是含幺交换环. 我们只需再证明 R/I 无零因子.

对于 $[a],[b]\in R/I$，如果有 $[a][b]=[0]$，即 $[ab]=[0]$. 这说明 $ab\in I$. 又 I 是环 R 的素理想，所以有

$$a\in I \text{ 或 } b\in I.$$

从而

$$[a]=[0] \text{ 或 } [b]=[0].$$

也就是，如果 $[a][b]=[0]$，则 $[a]=[0]$ 或 $[b]=[0]$. 这就证明了 R/I 无零因子. 又 R/I 是含幺交换环，所以它是整环.

3.4　商域(分式域)

3.3 节给出了由一个环得到域的一种构造方法，本节介绍第二种构造域的方法.

我们知道所有的整数关于数的普通加法和乘法构成一个环，而有理数集合却构成了一个域，并且整数环是有理数域的子环. 现在看看这个情况能否推广到一般，就是给了一

个环 R，可否找到一个除环或域包含这个环 R. 因为除环或域没有零因子，所以一个环 R 要能被一个除环或域包含，有一个必要条件，就是环 R 不能有零因子. 当 R 是非交换环时，这个条件还不充分，因为有例子说明了：一个无零因子的非交换环不一定能被一个除环包含. 但是当 R 是交换环时，这个条件就充分了. 也就是一个交换环一定可以扩充成域. 这种构造域的方法类似于由整数环得到有理数域的方法.

简单地说，这节要解决的主要问题是：R 为一个无零因子交换环，如何将其扩充为一个域，即如何找到域 Q，使 $R\subseteq Q$.

为此，我们先研究环的扩充.

3.4.1 环的扩充

首先需要解决问题是，如果环 S 与环 $\overline{S}$ 同构，S 是环 R 的子环，且 $R\backslash S$ 与 $\overline{S}$ 不相交，如何找到与 R 同构的环 $\overline{R}$，使 $\overline{S}$ 为 $\overline{R}$ 的子环.

引理 3.4.1 若集合 A 与集合 $\overline{A}$ 之间存在一个一一映射 f，并且 A 中有运算 $+$ 和 $\cdot$（称之为加法和乘法），则在 $\overline{A}$ 中可规定运算 $\overline{+}$ 和 $\overline{\cdot}$，使得 $\forall a,b\in A$，有

$$f(a+b)=f(a)\overline{+}f(b),$$

$$f(a\cdot b)=f(a)\,\overline{\cdot}\,f(b).$$

这样的映射 f 称为集合 A 与 $\overline{A}$ 间的关于加法和乘法的同构映射.

证明 因为 f 为一个一一映射，所以 $\overline{A}=f(A)=\{f(a)\mid a\in A\}$，且

$$f(a)=f(b)\Leftrightarrow a=b.$$

在 $\overline{A}$ 规定：

$$f(a)\overline{+}f(b)=f(a+b),$$

$$f(a)\,\overline{\cdot}\,f(b)=f(a\cdot b).$$

在上述规定下，f 为 A 与 $\overline{A}$ 的同构映射.

为简单起见，下面将 $\overline{A}$ 的运算亦记为 $+$ 和 $\cdot$.

定理 3.4.1 （挖补定理）设 S 是环 R 的子环，$R\backslash S$ 与另一个环 $\overline{S}$ 不相交（$(R\backslash S)\cap\overline{S}=\varnothing$）且 $S\cong\overline{S}$，则存在与 R 同构的环 $\overline{R}$，使 $\overline{S}$ 为 $\overline{R}$ 的子环.

证明 令 $\overline{R}=\overline{S}\cup(R\backslash S)$，设 φ 为 S 到 $\overline{S}$ 的同构映射（关于 S 到 $\overline{S}$ 中的加法和乘法）. 定义映射 $f:R\to\overline{R}$ 如下：

$$当\ a\in S\ 时，f(a)=\varphi(a),$$

$$当\ a\in R/S\ 时，f(a)=a.$$

易知 f 是满射，下面证明 f 是单射.

$\forall a,b\in R, a\neq b$，若 $a,b\in S$，则 $\varphi(a)\neq\varphi(b)$，故 $f(a)\neq f(b)$.

若 $a,b\notin S$，则 $f(a)=a\neq b=f(b)$.

若 $a\in S, b\notin R\backslash S$，则 $f(a)=\varphi(a)\in\overline{S}$，$f(b)=b\in R\backslash S$. 因为 $R\backslash S$ 与 $\overline{S}$ 不相交，故 $f(a)\neq f(b)$.

综上，f 为 R 到 $\overline{R}$ 的一一映射.

由引理 3.4.1，可在 $\overline{R}$ 中定义加法与乘法，使 R 与 $\overline{R}$ 关于各自的运算同构，余下只需说明 $\overline{S}$ 中原有的运算与 $\overline{S}$ 作为 $\overline{R}$ 的子集的运算是一致的. 事实上，由引理 3.4.1 的证明可知

$$\overline{S}=f(S)=\varphi(S).$$

新规定的加法和乘法为：$\forall f(a), f(b)\in\overline{S}$，有

$$f(a)+f(b)=f(a+b),$$
$$f(a)\cdot f(b)=f(a\cdot b).$$

而原有的加法和乘法为

$$\varphi(a)+\varphi(b)=\varphi(a+b),$$
$$\varphi(a)\cdot\varphi(b)=\varphi(a\cdot b).$$

可见两者是一致的.

3.4.2　商域

定理 3.4.2　每一个无零因子的交换环都是一个域的子环.

证明　设 R 为无零因子的交换环，且 $R\neq\{0\}$（R 为零环时定理显然是对的），下面分 4 个步骤证明.

(1) 令

$$A=\left\{\text{符号}\frac{a}{b}\,\middle|\,b\neq 0, a,b\in R\right\},$$

在 A 中规定关系～为

$$\frac{a}{b}\sim\frac{a'}{b'}\Leftrightarrow ab'=a'b,$$

则～是等价关系.

事实上，～满足自反性和对称性. 又

$$\frac{a_1}{b_1}\sim\frac{a_2}{b_2}, \frac{a_2}{b_2}\sim\frac{a_3}{b_3}\Rightarrow a_1b_2=a_2b_1,\ a_2b_3=b_2a_3\Rightarrow a_1b_2a_2b_3=a_2b_1b_2a_3\Rightarrow(a_1b_3-a_3b_1)a_2b_2=0,$$

若 $a_2=0$，则 $a_3=0$，否则 $a_1b_3-a_3b_1=0$，总之$\frac{a_1}{b_1}\sim\frac{a_3}{b_3}$，即满足传递性.

(2) 上述等价关系将 A 分成若干类.

令

$$Q_0=\left\{\text{所有类}\left[\frac{a}{b}\right]\right\},$$

在 Q_0 中规定：

$$\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]=\left[\frac{ad+bc}{bd}\right],$$

$$\left[\frac{a}{b}\right]\cdot\left[\frac{c}{d}\right]=\left[\frac{ac}{bd}\right].$$

首先证明这是两个代数运算，即若

$$\left[\frac{a}{b}\right]=\left[\frac{a'}{b'}\right],\ \left[\frac{c}{d}\right]=\left[\frac{c'}{d'}\right],$$

则有

$$\left[\frac{ad+bc}{bd}\right]=\left[\frac{a'd'+b'c'}{b'd'}\right],\tag{3.1}$$

并且

$$\left[\frac{ac}{bd}\right]=\left[\frac{a'c'}{b'd'}\right].\tag{3.2}$$

由

$$\left[\frac{a}{b}\right]=\left[\frac{a'}{b'}\right]\Rightarrow ab'=a'b,\tag{3.3}$$

由

$$\left[\frac{c}{d}\right]=\left[\frac{c'}{d'}\right]\Rightarrow cd'=c'd,\tag{3.4}$$

式(3.3)与式(3.4)相乘得到 $acb'd'=a'c'bd\Rightarrow$式(3.2)成立，

式(3.3)$\times dd'+$式(3.4)$\times bb'\Rightarrow$式(3.1)成立.

显然 Q_0 关于加法构成交换群，零元是$\left[\frac{0}{d}\right]$，$\left[\frac{a}{b}\right]$的负元是$\left[\frac{-a}{b}\right]$.

(3) Q_0 的全体非零元对乘法构成交换群.

设$\left[\frac{a}{b}\right]\neq[0]$（注意此时 $a\neq0$，因为若 $a=0$，则$\left[\frac{a}{b}\right]=[0]$），于是：

$$\left[\frac{a}{b}\right]\left[\frac{a}{a}\right]=\left[\frac{aa}{ba}\right]=\left[\frac{a}{b}\right],$$

$$\left[\frac{a}{b}\right]\left[\frac{b}{a}\right]=\left[\frac{ab}{ba}\right]=\left[\frac{a}{a}\right].$$

$\left[\frac{a}{a}\right]$是乘法的单位元，$\left[\frac{a}{b}\right]$的逆元是$\left[\frac{b}{a}\right]$.

容易验证 Q_0 中的(非)零元关于乘法满足封闭性、结合律和交换律. 也就是说 Q_0 的全体非零元对乘法构成交换群.

进一步，Q_0 是一个域(注意，R 中未必有幺元 1，因此不一定有[1]).

(4) 令

$$R_0=\left\{\left[\frac{qa}{q}\right] \mid q \text{ 为固定非零元}, a \text{ 为 } R \text{ 中任意元素}\right\}.$$

规定映射 $f:R\to R_0$ 为

$$r\to\left[\frac{qr}{q}\right], \forall r\in R,$$

则显然 f 为满射.

下面再证明 f 为单射.

若 $r_1\neq r_2$，则 $f(r_1)\neq f(r_2)$，否则即有

$$\left[\frac{qr_1}{q}\right]=\left[\frac{qr_2}{q}\right],$$

也就是

$$qr_1\cdot q=qr_2\cdot q,$$

于是得到 $r_1=r_2$.

又

$$f(r_1+r_2)=\left[\frac{q(r_1+r_2)}{q}\right]=\left[\frac{qr_1+qr_2}{q}\right]=\left[\frac{qr_1}{q}\right]+\left[\frac{qr_2}{q}\right]=f(r_1)+f(r_2),$$

$$f(r_1r_2)=\left[\frac{q(r_1r_2)}{q}\right]=\left[\frac{qr_1}{q}\cdot\frac{qr_2}{q}\right]=\left[\frac{qr_1}{q}\right]\cdot\left[\frac{qr_2}{q}\right]=f(r_1)\cdot f(r_2),$$

因此 f 是同构映射，所以 $R\cong R_0$，$R_0\subseteq Q_0$，根据定理 3.4.1，存在环 Q，且 $Q\cong Q_0$，使 $R\subseteq Q$. 显然 Q 是域.

上面 $Q_0(Q)$的构造看起来很复杂，实际上并非如此. Q 既然是包含 R 的域，那么 R 的每一个非零元 b 在 Q 中都有逆元 b^{-1}，因而

$$ab^{-1}=b^{-1}a=\frac{a}{b}(a,b\in R,b\neq 0)$$

在 Q 中有意义. 其实 Q 的结构也恰为

$$\{ab^{-1}\mid a,b\in R,b\neq 0\}.$$

定理 3.4.3　设 $Q=\{ab^{-1}\mid a,b\in R,b\neq 0\}$，$Q_0=\left\{\left[\frac{a}{b}\right]\mid a,b\in R,b\neq 0\right\}$，则 Q 与 Q_0

同构.

证明　定义映射 $f:Q\to Q_0$ 为

$$ab^{-1}\to\left[\frac{a}{b}\right],$$

则 f 为 Q 到 Q_0 的满射.

若

$$\left[\frac{a}{b}\right]=\left[\frac{a'}{b'}\right](b,b'\neq 0)\Rightarrow ab'=a'b\Rightarrow ab^{-1}=a'b'^{-1},$$

即 f 为单射. 又

$$f(ab^{-1}+cd^{-1})=f(adb^{-1}d^{-1}+cbb^{-1}d^{-1})=f((ad+cb)b^{-1}d^{-1})$$

$$=\left[\frac{ad+bc}{bd}\right]=\left[\frac{a}{b}\right]+\left[\frac{c}{d}\right]=f(ab^{-1})+f(cd^{-1})$$

$$f(ab^{-1}cd^{-1})=f(acb^{-1}d^{-1})=\left[\frac{ac}{bd}\right]=\left[\frac{a}{b}\right]\left[\frac{c}{d}\right]=f(ab^{-1})f(cd^{-1}).$$

综上所述 Q 与 Q_0 同构.

另外还有

$$\left[\frac{a}{b}\right]=\left[\frac{q^2a}{q^2b}\right]=\left[\frac{qa}{q}\right]\left[\frac{q}{qb}\right]=\left[\frac{qa}{q}\right]\left[\frac{qb}{q}\right]^{-1}.$$

注意到:$ab^{-1}\triangleq\frac{a}{b}$,则有以下计算性质:

$$\frac{a}{b}=\frac{c}{d}\Leftrightarrow ad=bc,$$

$$\frac{a}{b}+\frac{c}{d}=\frac{ad+bc}{bd},$$

$$\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}.$$

可以看出 Q 和 R 的关系恰好与有理数域与整数(偶数)环的关系一样,Q 的构造并不复杂.

定义 3.4.1　设 R 是无零因子的交换环,令

$$Q=\left\{\frac{a}{b}\mid a,b\in R,b\neq 0\right\},$$

则 Q 是包含 R 的一个域,称为环 R 的商域(分式域).

由定理 3.4.2 和定理 3.4.3,有两个以上元素的没有零因子的交换环至少有一个商域.

包含 R 的域可能不止一个，下面我们将证明包含 R 的域都以 R 的商域为子域.

定理 3.4.4　设 R 是一个至少有两个元的环，F 是包含 R 的域，则 F 也包含 R 的一个商域.

证明　设 F 是包含 R 的域，记

$$ab^{-1}=b^{-1}a=\frac{a}{b},\quad a,b\in R,b\neq 0,$$

做 F 的子集

$$\overline{Q}=\left\{\frac{a}{b}\mid a,b\in R,b\neq 0\right\}.$$

显然 $\overline{Q}$ 是 R 的一个商域.

定理 3.4.4 说明商域是包含 R 的最小域. 环的商域可能不止一个，但它们满足计算性质，而这些计算性质完全取决于 R 的加法和乘法，这也就是说，环 R 的商域完全取决于 R 的构造. 所以可以得到：

定理 3.4.5　同构的环的商域也同构，即一个环最多只有一个商域.

3.5　唯一分解环

整数环中每一个整数(不包括 0 和 1)都可以唯一分解成素数的乘积；数域上每一个次数大于零的多项式，都可以唯一分解成不可约多项式的乘积. 我们将整数环和多项式环的因子(式)分解的概念推广到一般的整环上. 本节主要讨论整环上的因式分解理论.

3.5.1　基本概念

首先将初等代数中的整除、因子或因式、倍数或倍式、素数的概念推广整环上.

定义 3.5.1　设 R 是整环，a,b,p,ε 均是 R 中的元素.

若存在元素 $c\in R$，使得 $b=ac$，就称 a 整除 b，记作 $a\mid b$，也称 a 是 b 的因子，b 是 a 的倍式. 否则记为 $a\nmid b$.

称 R 中有逆元的元素为单位.

若存在单位 ε，使得 $b=\varepsilon a$，称 b 为 a 的相伴元.

显然环中元素的相伴关系是一个等价关系，因此如果 b 为 a 的相伴元，a 也为 b 的相伴元. 易知两个元素相伴的充分必要条件是它们互相整除.

如果 a 是 R 的非零元，则有 $a=\varepsilon(\varepsilon^{-1}a)$，其中 ε 是单位，可见单位和 a 的相伴元一定是 a 的因子. 称这两类因子为 a 的平凡因子，其余的因子（如果还有的话）称为 a 的真因子.

例 3.5.1 求出 Gauss 整环 $Z[\mathrm{i}]$ 中所有的单位以及整数 5 的所有真因子.

解 设 $\varepsilon=a+b\mathrm{i}$ 是 $Z[\mathrm{i}]$ 中的任一单位，则有 $\eta\in Z[\mathrm{i}]$，使得

$$\varepsilon\eta=1,\ |\varepsilon|^2|\eta|^2=1.$$

这里只能有 $|\varepsilon|^2=a^2+b^2=1$，从而只有

$$a=\pm1, b=0 \quad \text{或}\ a=0,\ b=\pm1.$$

即 ε 只能是 ±1 及 $\pm\mathrm{i}$. 因此 ±1 和 $\pm\mathrm{i}$ 是 $Z[\mathrm{i}]$ 中的全部单位.

设 $\alpha=a+b\mathrm{i}$ 是 5 在 $Z[\mathrm{i}]$ 中的任一真因子，则存在 $\beta\in Z[\mathrm{i}]$，使

$$5=\alpha\beta,$$

从而

$$|\alpha|^2|\beta|^2=25,$$

这里只能有 $|\alpha|^2=1,5$ 或 25.

因为 α 是 5 的真因子，所以 $|\alpha|^2\neq1,25$. 否则：如果 $|\alpha|^2=1$，α 是单位；如果 $|\alpha|^2=25$，则 $|\beta|^2=1$，β 是单位，从而 α 是 5 的相伴元. 这都与 α 是 5 的真因子矛盾，所以只能有

$$|\alpha|^2=a^2+b^2=5.$$

解此方程得 $\begin{cases}a=\pm1\\ b=\pm2\end{cases}$ 或 $\begin{cases}a=\pm2\\ b=\pm1\end{cases}$.

于是 5 的真因子只有 8 个，分别是

$$\pm1\pm2\mathrm{i},\pm2\pm\mathrm{i}.$$

定义 3.5.2 设 R 是整环，a,b 均是 R 中的元素.

如果 a 是 R 的非零元，a 不是单位，而且 a 没有真因子，则称 a 为不可约元素或既约元，否则称 a 为可约元.

如果 p 是 R 的非零元，p 不是单位，而且当 $p|ab$ 时，有 $p|a$ 或 $p|b$，则称 p 为素元.

例如，在整数环中，全体素数是既约元也是素元. 但在 Gauss 整数环中，素数就不一定是既约元了. 例如，2 是素数，但 $2=(1+\mathrm{i})(1-\mathrm{i})$，而 $1+\mathrm{i}$ 和 $1-\mathrm{i}$ 都是不可逆的，即都不是单位，所以 2 不是既约元，显然 2 也不是素元. 下面的例子将说明在环 $Z[\sqrt{5}\mathrm{i}]$ 中，3 是既约元，但不是素元.

例 3.5.2 证明 3 在整环

$$Z[\sqrt{5}\mathrm{i}]=\{a+b\sqrt{5}\mathrm{i}\mid a,b\in Z\}$$

中是既约元,但不是素元.

证明　首先易知,$Z[\sqrt{5}\mathrm{i}]$中的单位只有± 1.

下面证明若$|\alpha|^2=9$,则α是既约元.

事实上,若$\beta=a+b\sqrt{5}\mathrm{i}$是$\alpha$的任一因子,则有$\gamma\in Z[\sqrt{5}\mathrm{i}]$,使得

$$\alpha=\beta\gamma,$$

从而

$$|\beta|^2|\gamma|^2=|\alpha|^2=9.$$

这里只能有$|\beta|^2=a^2+5b^2=1,3,9$,但易知$|\beta|^2=a^2+5b^2=3$不可能,故只有

$$|\beta|^2=a^2+5b^2=1 \text{ 或 } 9.$$

当$|\beta|^2=1$时,β是单位.

当$|\beta|^2=9$时,$|\gamma|^2=1$,即γ是单位,从而β是相伴元.

总之,α的因子或是单位或是相伴元,因此α只有平凡因子,所以α是既约元.

由此可知 3 和$2\pm\sqrt{5}\mathrm{i}$都是既约元.但由于

$$3\mid(2+\sqrt{5}\mathrm{i})(2-\sqrt{5}\mathrm{i}),$$

而 3 不能整除其中的任一个,所以 3 不是$Z[\sqrt{5}\mathrm{i}]$中的素元.

确定一个环中的所有既约元和素元不是容易的事.但素元和既约元有着非常密切的关系,一般我们有:

定理 3.5.1　在整环R中,素元一定是既约元.

证明　设p是素元,a是p的因子,即有非零元b,使得$p=ab$,由素元的定义可知$p\mid a$或$p\mid b$.若$p\mid a$,则a是p的相伴元.若$p\mid b$,则存在非零元c,使得$b=pc$,这样就有$p=ab=acp$,因为R中满足消去律,得$ac=1$,即a是单位.总之a是平凡因子,这说明p没有真因子,所以p是既约元.

由例 3.5.2 可以看出定理的逆是不对的,即既约元不一定是素元.

定义 3.5.3 若整环R中的既约元都是素元,则称R满足素性条件.

3.5.2　唯一分解环

为叙述简单,用符号R^*表示R中非零元,而符号U表示R中的所有单位构成的集合.

定理 3.5.2　设R是整环,元素$a\in R^*-U$,则a是可约元的充分必要条件是存在b,$c\in R^*-U$,使得$a=bc$.

证明 必要性. a 是可约元素,故 a 有真因子 b,即存在 $c\in R^*$,使 $a=bc$,显然 $b\in R^*-U$. 易知 $c\notin U$,否则 b 是 a 的相伴元,与 b 是真因子矛盾.

充分性. 若存在 $b,c\in R^*-U$,使 $a=bc$,则 b 不是 a 的相伴元. 否则存在 $u\in U$,使

$$b=ua,\ a=bc=uac,$$

即

$$uc=1.$$

这与 $c\notin U$ 相矛盾.

这样,b 不是 a 的相伴元,又不是单位,所以 b 是 a 的真因子,从而 a 是可约元.

下面我们讨论整环里的因式分解理论.

定义 3.5.4 如果

(1) $a=p_1p_2\cdots p_r$,$p_i(1\leqslant i\leqslant r)$是 R 的既约元;

(2) 若同时有 $a=q_1q_2\cdots q_s$,$q_j(1\leqslant j\leqslant s)$是 R 的既约元,那么 $r=s$,适当调整 q_i 的次序后,有 $q_i=\varepsilon_i p_i$(ε_i 是单位,$1\leqslant i\leqslant s$).

则称整环 R 的元 a 有唯一分解.

因为零元不是既约元,整环又没有零因子,故零元不能表示成既约元的乘积. 同样单位也不能表示成既约元的乘积. 因此在整环中,零元和单位当然都不能唯一分解. 但是判断其它元素能否唯一分解,也是很困难的,有时甚至是不可解决的. 即使我们要判断一个元素是否是既约元,有时也是不容易的. 例如,要判断环 $F[x]$中的多项式是否不可约就比较困难. 但是对有些环中的有些元素来说,就容易些.

例如,在 $Z(\sqrt{5}\mathrm{i})$中 3 和 $2\pm\sqrt{5}\mathrm{i}$ 都是既约元,

$$9=3\times 3=(2+\sqrt{5}\mathrm{i})(2-\sqrt{5}\mathrm{i}),$$

3 又不与 $2\pm\sqrt{5}\mathrm{i}$ 中的任一个相伴,可见 9 不能进行唯一分解.

定义 3.5.5 在整环 R 中,如果对任意的元素 a,当 a 不是零元,又不是单位时,它就有唯一分解,则称 R 是唯一分解环.

下面讨论唯一分解环的性质. 由前面的讨论知道,素元一定是既约元,但既约元不一定是素元. 可是在整数环和域上的多项式环中,素元和既约元是一致的. 我们将这个结论推广到一般的唯一分解环上.

定理 3.5.3 设 R 是唯一分解环,p 是 R 的既约元,则 p 是 R 的素元. 即唯一分解环满足素性条件.

证明 设 p 是 R 的既约元,如果

$$p\mid ab,$$

其中 a,b 为 R 中的元素. 也就是存在 $c\in R^*$，使

$$cp=ab.$$

若 $a=0$ 或 $b=0$，则 $p\mid a$ 或 $p\mid b$.

若 $a\in U$，则 ab 是 b 的相伴元，所以 $p\mid b$.

若 $b\in U$，则 $p\mid a$.

以下对 $a,b\in R^*-U$ 讨论，设 $cp=ab$，则 $c\notin U$.

事实上，如果 $c\in U$，即 c 是单位，那么 cp 就是 p 的相伴元. 易知，既约元的相伴元也是既约元，从而 cp 也是既约元. 而 $a,b\in R^*-U$，说明 a,b 是 cp 的真因子，这是一个矛盾. 于是 $c\notin U$，即 $c\in R^*-U$.

设

$$c=p_1p_2\cdots p_n,a=q_1q_2\cdots q_r,b=\tilde{q}_1\tilde{q}_2\cdots\tilde{q}_s,$$

其中 $p_i(1\leqslant i\leqslant n),q_j(1\leqslant j\leqslant r),\tilde{q}_k(1\leqslant k\leqslant s)$是既约元，则有

$$pp_1p_2\cdots p_n=q_1q_2\cdots q_r\tilde{q}_1\tilde{q}_2\cdots\tilde{q}_s.$$

由分解的唯一性可知，p 必定是某个 q_i 或$\tilde{q}_j$的相伴元，因此 $p\mid a$ 或 $p\mid b$.

在一定意义上，上述定理的逆定理也是成立的，它也是判断唯一分解环的依据.

定理 3.5.4　若整环 R 满足：

(1) $\forall a\in R^*-U$，a 可分解为有限个既约元的乘积；

(2) R 满足素性条件.

则 R 是唯一分解环.

证明　由(1)可知，存在既约元 $p_1,p_2,\cdots,p_r$，使 $a=p_1p_2\cdots p_r$.

若另有分解式 $a=q_1q_2\cdots q_s$，q_i 为既约元，$i=1,2,\cdots,s$，则

$$p_1p_2\cdots p_r=q_1q_2\cdots q_s.$$

对 r 用数学归纳法来证明分解的唯一性.

当 $r=1$ 时，若 $s\neq1$，则 p_1 有真因子 q_1，与 p_1 为既约元矛盾.

假设 $r\leqslant k-1$ 时，分解的唯一性成立.

当 $r=k$ 时，由

$$p_1p_2\cdots p_k=q_1q_2\cdots q_s,$$

得

$$p_1\mid q_1q_2\cdots q_s,$$

故

$$p_1 \mid \text{某个 } q_{i_0},$$

不妨设 $i_0=1$(调换次序以后)，于是 $q_1=\varepsilon_1 q_1$ 是 p_1 的相伴元，其中 $\varepsilon_1\in U$.

而

$$p_2\cdots p_k=\varepsilon_1 q_2\cdots q_s=\widetilde{q}_2\cdots q_s,$$

由归纳假设可知 $k-1=s-1$，且 $q_i=\varepsilon_i p_i$ 为 q_i 的相伴元，其中 $2\leqslant i\leqslant k$. 于是得到 $k=s$，且 $q_i=\varepsilon_i p_i$，$1\leqslant i\leqslant k$.

整数环中的最大公因数和数域 F 上多项式环 $F[x]$ 中的最大公因式的概念和讨论，也可以在唯一分解环中得到推广.

定义 3.5.6 如果整环 R 中的元素 c 是 $a_1,a_2,\cdots,a_n$ 的因子，则称 c 是这 n 个元素的公因子. 如果 d 是 $a_1,a_2,\cdots,a_n$ 的一个公因子，而且 $a_1,a_2,\cdots,a_n$ 的任何公因子都是 d 的一个因子，则称 d 是 $a_1,a_2,\cdots,a_n$ 的最大公因子.

定理 3.5.6 设 R 为唯一分解环，则 R 中任意两个元素都有最大公因子存在，且最大公因子之间只差一个单位因子.

证明 对于 R 中任意两个元素 a,b，若 $a=0$，则显然 b 是 a 与 b 的一个最大公因子；若 a 是单位，则显然 a 就是 a 与 b 的一个最大公因子. 因此，下面设 a 与 b 既不是零元也不是单位.

设

$$a=q_1q_2\cdots q_r,\quad b=q_1'q_2'\cdots q_s'$$

为 a 与 b 的因子分解，其中 q_i,q_j' 为素元，且假定 $p_1,p_2,\cdots,p_n$ 是

$$q_1,q_2,\cdots,q_r,q_1',q_2',\cdots,q_s',$$

中互不相伴的素元，而其中别的元素都同某个 $p_i(1\leqslant i\leqslant n)$ 相伴. 这样，

a 与 b 可表示为

$$a=\varepsilon_a p_1^{t_1}p_2^{t_2}\cdots p_n^{t_n},b=\varepsilon_b p_1^{k_1}p_2^{k_2}\cdots p_n^{k_n},$$

其中 $\varepsilon_a,\varepsilon_b$ 是单位，而 $t_i,k_j(1\leqslant i,j\leqslant n)$ 是非负整数.

令 $l_i=\min\{t_i,k_i\}$，$1\leqslant i\leqslant n$，且

$$d=p_1^{l_1}p_2^{l_2}\cdots p_n^{l_n},$$

则显然 d 是 a 与 b 的一个公因子.

又假定 c 是 a 与 b 的任一个公因子，若 c 是单位，则当然 $c\mid d$；若 c 不是单位，则令

$$c=p_1'p_2'\cdots p_t',p_i'\text{是素元},1\leqslant i\leqslant t.$$

由于 $c\mid a$，故每个 $p_i'\mid a$，从而 p_i'整除某个 p_j. 但二者都是素元，故相伴. 这样可设

$$c=\varepsilon_c p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n},$$

其中 ε_c 是单位，m_i 是非负整数. 由于 $c|a$，且 p_i 与 $p_j(i\neq j)$互不相伴，故 $m_i\leqslant t_i$.

同理可得 $m_i\leqslant k_i$. 因此 $m_i\leqslant l_i$，从而 $c|d$，即 d 是 a 与 b 的一个最大公因子.

假定 d' 也是 a 与 b 的一个最大公因子，则易知 d 与 d' 互相整除，从而二者相伴.

利用数学归纳法可进一步推广这个定理.

推论 3.5.1　唯一分解环 R 中的元素 $a_1,a_2,\cdots,a_n$ 在 R 中有最大公因子存在，而且其任意两个最大公因子均相伴.

定义 3.5.7　如果唯一分解环 R 中的元素 $a_1,a_2,\cdots,a_n$ 的最大公因子是单位，则称这 n 个元素互素，并记为$(a_1,a_2,\cdots,a_n)=1$.

关于元素的互素有以下结论：

定理 3.5.4　在唯一分解环 R 中，如果 $a|bc$，$(a,b)=1$，则 $a|c$.

请读者自己证明.

3.6　主理想整环和欧氏环

本节讨论两类唯一分解环——主理想整环和欧氏环，这两类环在环论中也起着非常重要的作用.

3.6.1　主理想整环

定义 3.6.1　如果整环 R 的每一个理想都是主理想，则称 R 为主理想整环.

设 Z 是整数环，则 Z 的全部理想为 $nZ(n\geqslant 0)$，因此整数环是主理想整环. 而 Z 上的多项式环 $Z[x]$不是主理想环，因为$(2,x)$不是主理想.

但应注意，虽然模 n 剩余类环 Z_n 的全部理想都是主理想，但是当 n 是合数时 Z_n 有零因子，所以 Z_n 不是主理想整环.

主理想整环是唯一分解环，为了证明这个结论，我们先证明两个引理，而这两个引理本身也是重要的结论.

引理 3.6.1　如果 R 是一个主理想整环，在序列

$$a_1,a_2,\cdots,a_n,\cdots,\quad a_i\in R$$

中，每个元素是前面元素的真因子，则这个序列是个有限序列.

证明　做主理想

$$(a_1),(a_2),\cdots,(a_n),\cdots,$$

由于 a_{i+1} 是 a_i 的因子，显然

$$(a_1)\subset(a_2)\subset\cdots\subset(a_n)\cdots.$$

令

$$N=\bigcup_{i=1,2,\cdots}(a_i),$$

则易知 N 是 R 的一个理想.

又 R 是主理想整环，所以 N 是主理想. 设

$$N=(d),d\in R,$$

由于 $d\in N$，所以 d 属于某个 (a_i). 如果 $d\in(a_m)$，则 a_m 是序列中的最后一个元素.

如若不然，假设在 a_m 后面还有元素 a_{m+1}，则由于

$$d\in(a_m),a_{m+1}\in N=(d),$$

有 $a_m|d,d|a_{m+1}$，所以 $a_m|a_{m+1}$，这与 a_{m+1} 是 a_m 的真因子矛盾.

引理 3.6.2 主理想整环中每一个既约元生成的理想是极大理想.

证明 设 R 是主理想整环，a 是环 R 的一个既约元，B 为 R 的任意理想，且满足

$$(a)\subseteq B\subseteq R.$$

因为 R 是主理想整环，所以存在 $b\in R$，使 $B=(b)$，于是 $b|a$，a 是既约元. 因此 b 或者是单位，或者是 a 的相伴元. 如果 b 是单位，则 $B=(b)=R$. 如果 b 是 a 的相伴元，则 $B=(b)=(a)$.

定理 3.6.1 主理想整环是唯一分解环.

证明 我们利用定理 3.5.4 证明.

设 R 是一个主理想整环，a 为 R 中的任意一个非单位的非零元.

首先证明 a 能够表示成有限个既约元的乘积.

用反证法. 如果 a 不能表示成有限个既约元的乘积，则 a 不是既约元. 设它的真因子为 a_1，则有

$$a=a_1b.$$

易知 b 也是 a 的真因子. 其中 a_1，b 至少有一个不能表示成有限个既约元的乘积，否则 a 就能够表示成有限个既约元的乘积了. 不妨设 a_1 不能表示成有限个既约元的乘积，则 a_1 不是既约元. 同样，a_1 又有真因子 a_2，而 a_2 不能表示成有限个既约元的乘积，等等. 如此下去，可得到一个无限序列

$$a,a_1,a_2,\cdots.$$

其中每个都是前一个的真因子，与引理 3.6.1 矛盾. 这说明 a 能够表示成有限个既约元的乘积.

再证明 R 中的既约元 p 是素元.

设 $p|ab$,则 $ab=rp\in(p)$,因此在商环 $R/(p)$ 中 $[ab]=[0]$. 由引理 3.6.2 可知,(p) 是极大理想,又 R 是含幺交换环,由定理 3.3.6 可知,$R/(p)$ 是域. 所以 $R/(p)$ 没有零因子. 由 $[ab]=[0]$ 得知或者 $[a]=[0]$,或者 $[b]=[0]$,从而 $p|a$ 或者 $p|b$,这说明 p 是素元.

综上,根据 3.5 节定理 3.5.4 证得主理想整环是唯一分解环.

下面我们介绍另一类唯一分解环——欧氏环.

3.6.2　欧氏环

定义 3.6.2　一个整环 I 叫做欧氏环,如果

(1) 有一个从 I 的非零元全体到非负整数集的映射

$$\phi: I^* \to \mathbf{Z}^+ \cup \{0\}.$$

(2) 取 $a\in I^*$, $\forall b\in I$,都有 $b=qa+r(q,r\in I)$,这里 $r=0$ 或 $\phi(r)<\phi(a)$

例 3.6.1　整数环 Z 是一个欧氏环.

证明 定义映射 $\phi:\mathbf{Z}^* \to \mathbf{Z}^+ \cup \{0\}$ 为

$$\phi: a \to |a| = \phi(a).$$

$\forall b\in Z$,取 $a\neq 0$,有

$$b=qa+r,$$

其中 $r=0$,或者 $\phi(r)=|r|<|a|=\phi(a)$. 所以整数环 Z 是一个欧氏环.

例 3.6.2　数域 F 上的多项式环 $F[x]$ 是一个欧氏环.

证明　令 $F[x]\backslash\{0\}$ 到非负整数集的映射 φ 为

$$f(x) \to f(x) \text{ 的次数}.$$

在 $F[x]$ 中任取 $f(x)$ 及 $g(x)\neq 0$,存在 $F[x]$ 中的多项式 $q(x)$,$r(x)$,满足

$$f(x)=g(x)q(x)+r(x),$$

其中 $r(x)=0$ 或 $r(x)$ 的次数小于 $g(x)$ 的次数.

定理 3.6.2　欧氏环是主理想整环,因而是唯一分解环.

证明　设 R 是一个欧氏环,δ 为 $R^*=R\backslash\{0\}$ 到非负整数集上的映射,I 是 R 的任意理想. 若 I 是零理想,则 I 是主理想.

设 $I\neq\{0\}$,取 $b\in I$,使

$$\delta(b)=\min\{\delta(c)\,|\,c\in I, c\neq 0\}.$$

设 $a\in I$,则有 $q,r\in R$,使 $a=qb+r$,故 $r=a-qb\in I$. 如果 $r\neq 0$,则

$$\delta(r)<\delta(b),$$

与 b 的选取矛盾. 因此 $r=0, a=qb$, 即 $I=(b)$, I 为主理想.

3.7 多项式环

多项式环在环论中起着非常重要的作用, 这一节我们首先将高等代数中数域上多项式推广到环上, 进一步讨论环上多项式的性质.

3.7.1 环上的一元多项式

设 R 是环, x 是一个文字, 称为未定元, i 是一个非负整数. 形如

$$a_i x^i,\ a\in R$$

的式子叫做系数在 R 中的未定元 x 的单项式. 形如

$$a_n x^n + a_{n-1}x^{n-1}+\cdots+a_1 x+a_0,\quad a_i\in R, i=1,2,\cdots,n$$

(其中 n 为任意非负整数)的式子称为系数在环 R 上未定元 x 的多项式, 简称环 R 上的(一元)多项式.

多项式中 $a_i x^i$ 叫做它的 i 次项, a_i 叫做 i 次项的系数. 如果 $a_i=0$, 通常在表达式中省略 $a_i x^i$ 这一项.

我们习惯用记号 $f(x), g(x)$ 来表示多项式.

设 $f(x)$ 和 $g(x)$ 是环 R 上的两个多项式, 如果它们同次项的系数都相等, 我们就说 $f(x)$ 和 $g(x)$ 相等, 记作 $f(x)=g(x)$.

下面我们定义多项式的两种运算.

设

$$f(x)=\sum_{i=0}^{n}a_i x^i,\quad g(x)=\sum_{j=0}^{m}b_j x^j,$$

令 $M=\max\{n,m\}$, 且

$$a_{n+1}=a_{n+2}=\cdots=a_M=0,$$

$$b_{m+1}=b_{m+2}=\cdots=b_M=0.$$

规定 $f(x), g(x)$ 的和为

$$f(x)+g(x)=\sum_{i=0}^{M}(a_i+b_i)x^i.$$

再令

$$a_{n+1}=a_{n+2}=\cdots=a_{n+m}=0,$$

$$b_{m+1}=b_{m+2}=\cdots=b_{n+m}=0.$$

规定 $f(x)$,$g(x)$的积为

$$f(x)g(x)=\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i}a_jb_{i-j}\right)x^i.$$

容易验证环 R 上的多项式关于上述的加法和乘法构成一个环.

定义 3.7.1 环 R 上的全体多项式关于多项式的加法和乘法构成一个环,称这个环为 R 上多项式环,记为 $R[x]$.

类似地,我们给出多元多项式的定义.

设 $x_1,x_2,\cdots,x_n$ 是 n 个文字,设 $R_1=R[x_1]$,$R_2=R_1[x_2]$,$\cdots$,$R_n=R_{n-1}[x_n]$.

形如

$$\sum_{i_1i_2\cdots i_n}a_{i_1i_2\cdots i_n}x_1^{i_1}x_2^{i_2}\cdots x_n^{i_n},\quad a_{i_1i_2\cdots i_n}\in R(\text{只有有限个 } a_{i_1i_2\cdots i_n} \text{ 非零}),$$

的式子叫做系数在环 R 上的 $x_1,x_2,\cdots,x_n$ 的多项式,简称 R 上的多元多项式.

类似地定义加法和乘法,多元多项式也构成一个环,称为多元多项环,记为 $R[x_1,x_2,\cdots,x_n]$.

定义 3.7.2 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 为环 R 上的多项式.如果 $a_n\neq 0$,称 a_n 是 $f(x)$ 的首项系数,a_0 是常数项,并称 n 是多项式 $f(x)$ 的次数,记作 $\deg(f(x))$.

当 $f(x)$ 的所有系数都是 0 时,称为零多项式,仍用 0 表示.规定零多项式的次数为 $-\infty$.次数$\leqslant 0$ 的多项式称为常多项式.如果 R 有单位元 1 且首项系数 $a_n=1$,$f(x)$就称为首一多项式.

通过计算两个多项式的和与积,我们得到:

定理 3.7.1 设 $f(x),g(x)\in R[x]$,则

$$\deg(f(x)+g(x))\leqslant\max\{\deg(f(x)),\deg(g(x))\},$$

$$\deg(f(x)g(x))\leqslant\deg(f(x))+\deg(g(x)).$$

如果 R 是整环,则有

$$\deg(f(x)g(x))=\deg(f(x))+\deg(g(x)).$$

我们如果将常多项式视为 R 中的元素,这样 R 就可以视为 $R[x]$的子环,由此 R 的一些性质可以推广到 $R[x]$上.

定理 3.7.2 设 R 是环，则有：

(1) $R[x]$是交换环当且仅当 R 是交换环；

(2) $R[x]$是有单位元的环当且仅当 R 是有单位元的环；

(3) $R[x]$是整环当且仅当 R 是整环.

3.7.2 域上的一元多项式

我们把系数在域 F 中的多项式称为域上的多项式. 从上面的定理容易看出，一个域上的多项式环 $F[x]$一定是整环.

定义 3.7.3 设 $f(x)$和 $g(x)$是域 F 上的任意两个多项式，$g(x)\neq 0$. 如果存在一个多项式 $q(x)\in F[x]$，使得

$$f(x)=q(x)g(x)$$

成立，则称 $g(x)$整除 $f(x)$，或者 $f(x)$被 $g(x)$整除，记作 $g(x)\mid f(x)$.

同时我们把 $g(x)$叫做 $f(x)$的因式，而把 $f(x)$叫做 $g(x)$的倍式.

显然，任意一个多项式，一定有两类因式，一类是非零的常多项式，另一类是多项式本身. 我们把这两类因式称为多项式的平凡因式，否则就称为非平凡因式.

如果一个多项式不能写成两个非平凡因式的乘积，我们就称这个多项式是不可约多项式，或既约多项式.

不可约多项式在多项式环乃至域论中都起着非常重要的作用，后面的定理可以看到 $F[x]$中的每一个多项式都可以分解成不可约多项式的乘积. $F[x]$上多项式也有类似数域上的多项式的性质.

定理 3.7.3 （多项式带余除法）对于 $F[x]$中的任意两个多项式 $f(x)$和 $g(x)$，其中 $g(x)\neq 0$，一定存在 $F[x]$中的多项式 $q(x)$和 $r(x)$，满足

$$f(x)=q(x)g(x)+r(x),$$

其中 $\deg(r(x))<\deg(g(x))$.

证明 如果 $\deg(f(x))<\deg(g(x))$，取 $q(x)=0, r(x)=f(x)$，则定理成立.

下面假设 $\deg(f(x))\geqslant\deg(g(x))$，并设 $f(x)$和 $g(x)$的次数分别为 n, m. 对 $f(x)$的次数作(第二)数学归纳法.

假设对次数小于 n 的多项式，结论成立. 现在考查 n 次多项式情况.

令 ax^n, bx^m 分别表示多项式 $f(x)$和 $g(x)$的首项，多项式

$$f_1(x)=f(x)-b^{-1}ax^{n-m}g(x)$$

的次数小于 n. 由归纳法假设，对 $f_1(x), g(x)$存在 $q_1(x)$和 $r_1(x)$，使

$$f_1(x)=q_1(x)g(x)+r_1(x),$$

且 $\deg(r_1(x))<\deg(g(x))$. 于是

$$f(x)=(q_1(x)+b^{-1}ax^{n-m})g(x)+r_1(x).$$

即有

$$q(x)=q_1(x)+b^{-1}ax^{n-m},\quad r(x)=r_1(x)$$

使

$$f(x)=q(x)g(x)+r(x)$$

成立.

由数学归纳法,对任意的 $f(x)$ 和 $g(x)\neq 0$,多项式 $q(x)$ 和 $r(x)$ 存在性就证明了.

例 3.7.1　$f(x)=2x^5+x^4+4x+3\in F_5[x]$,$g(x)=3x^2+1\in F_5[x]$,有

$$f(x)=(4x^3+2x^2+2x+1)g(x)+2x+2.$$

定理 3.7.4　设 F 是域,那么 F 上的多项式 $F[x]$ 是主理想整环. 即对任意的非零理想 J,存在多项式 $g(x)\in F[x]$,使得 $J=(g(x))$.

证明　因为 $J\neq\{0\}$,因此 J 中一定存在非零多项式. 假设 $g(x)$ 是 J 中次数最低的多项式,下面证明 $g(x)$ 是 J 的一个生成元.

设 $f(x)$ 是 J 中的任意一个元素,则根据定理 3.7.3,一定存在 $q(x)$ 和 $r(x)\in F[x]$ 使得

$$f(x)=q(x)g(x)+r(x),\deg(r(x))<\deg(g(x)).$$

又因为 J 是理想,$g(x)\in J$,所以 $q(x)g(x)\in J$,从而

$$r(x)=f(x)-q(x)g(x)\in J,$$

并且 $\deg(r(x))<\deg(g(x))$.

但是根据假设,$g(x)$ 是 J 中次数最低的多项式,因此 $r(x)=0$,也就是说 $f(x)=q(x)g(x)$,所以 $J=(g(x))$.

定义 3.7.4　假设 $f_1(x)$,$f_2(x)$ 是 $F[x]$ 中多项式,$F[x]$ 中的多项式 $d(x)$ 称为 $f_1(x)$,$f_2(x)$ 的一个最大公因式,如果它满足下面两个条件:

(1) $d(x)$ 是 $f_1(x)$,$f_2(x)$ 的公因式;

(2) 若 $c(x)\in F[x]$ 也是它们的公因式,则 $c(x)$ 整除 $d(x)$.

公因式和最大公因式的概念很容易推广到有限个多项式上,下面证明若干个多项式的最大公因式的存在性、性质和求法.

定理 3.7.5　假设 $f_1(x),f_2(x),\cdots,f_n(x)$ 是 $F[x]$ 中的一组多项式,则 $F[x]$ 中存在它们的最大公因式 $d(x)$,并且更进一步,存在 $b_1(x),b_2(x),\cdots,b_n(x)\in F[x]$ 使得

$$d(x)=\sum_{i=1}^{n}b_i(x)f_i(x).$$

证明 令 $J=\left\{\sum_{i=1}^{n}c_i(x)f_i(x)\mid c_i(x)\in F[x]\right\}$，则 J 是 $F[x]$ 中的理想，且 $f_i(x)\in J$. 由于 $F[x]$ 是主理想整环，所以存在多项式 $d(x)\in F[x]$，使 $J=(d(x))$，所以 $d(x)$ 整除每个多项式 $f_1(x),f_2(x),\cdots,f_n(x)$.

假设 $d_1(x)$ 也整除 $f_1(x),f_2(x),\cdots,f_n(x)$，则对于 $F[x]$ 任意的多项式

$$c_1(x),c_2(x),\cdots,c_n(x),$$

有

$$d_1(x)\mid c_1(x)f_1(x)+c_2(x)f_2(x)+\cdots+c_n(x)f_n(x).$$

也就是 $d_1(x)$ 能写成 $f_1(x),f_2(x),\cdots,f_n(x)$ 的组合形式，从而 $d_1(x)\in J$，所以 $d_1(x)\mid d(x)$.

又因为 $d(x)\in J$，所以存在多项式 $b_1(x),b_2(x),\cdots,b_n(x)\in F[x]$，使

$$d(x)=\sum_{i=1}^{n}b_i(x)f_i(x).$$

容易看出 $f_1(x),f_2(x),\cdots,f_n(x)$ 的首一最大公因式是唯一的，记为

$$(f_1(x),f_1(x),\cdots,f_n(x)).$$

如果 $(f_1(x),f_1(x),\cdots,f_n(x))=1$，则称多项式 $f_1(x),f_2(x),\cdots,f_n(x)$ 互素.

关于互素多项式有以下性质.

定理 3.7.6 设 $f(x),g(x),h(x)\in F[x]$，$h(x)\mid f(x)g(x)$，那么如果 $(h(x),f(x))=1$，则 $h(x)\mid g(x)$.

证明 根据定理 3.7.5，存在多项式 $s(x),t(x)\in F[x]$，使

$$s(x)f(x)+t(x)h(x)=1$$

两边同时乘以 $g(x)$，得

$$\begin{aligned}g(x)&=s(x)f(x)g(x)+t(x)h(x)g(x)\\&=s(x)(f(x)g(x))+h(x)(t(x)g(x)).\end{aligned}$$

因为 $h(x)$ 整除上式右边的每一项，因此 $h(x)$ 也整除上式的左边，即 $h(x)\mid g(x)$.

类似于高等代数中数域上多项式的最大公因式的方法——辗转相除法，我们可以求得 $F[x]$ 中多项式的最大公因式.

相对于多项式的最大公因式，我们也可以定义多项式的最小公倍式.

定义 3.7.5 设 $f(x),g(x)\in F[x]$，$m(x)$ 是域 F 上的另一个多项式. 如果

(1) $f(x)\mid m(x)$，$g(x)\mid m(x)$；

(2) 对于 $h(x)\in F[x]$,如果也有 $h(x)\mid f(x)$,$h(x)\mid g(x)$,则 $m(x)\mid h(x)$.

那么 $m(x)$就叫做 $f(x)$和 $g(x)$的最小公倍式,记作$[f(x),g(x)]$,或 $\mathrm{lcm}(f(x),g(x))$.

定理 3.7.7 设 $p(x)$是 $F[x]$中的一个多项式,由 $p(x)$生成的理想为$(p(x))$,则

$$(p(x))\text{是 }F[x]\text{中的极大理想}\Leftrightarrow p(x)\text{是不可约多项式}.$$

证明 充分性. 设 $p(x)$是 $F[x]$中的不可约多项式.

假设 J 是 $F[x]$的一个理想,且$(p(x))\subseteq J$. 如果 $J\neq(p(x))$,则只需要证明 $J=F[x]$.

取多项式 $r(x)\in J$,但 $r(x)\notin(p(x))$. 因为 $p(x)$是一个不可约多项式,所以

$$(p(x),r(x))=1 \text{ 或 } (p(x),r(x))=p(x).$$

但由于 $r(x)\notin(p(x))$,因此 $p(x)\nmid r(x)$,从而$(p(x),r(x))\neq p(x)$,所以

$$(p(x),r(x))=1.$$

根据定理 3.7.6,存在多项式 $s(x),t(x)\in F[x]$,使得

$$s(x)p(x)+t(x)r(x)=1.$$

但 $p(x),r(x)\in J$,因此

$$s(x)p(x)+t(x)r(x)=1\in J,$$

所以 $J=F[x]$. 这样就证明了$(p(x))$是极大理想.

必要性. 设$(p(x))$是 $F[x]$中的极大理想,$p(x)$是 $F[x]$中可约多项式. 令

$$p(x)=p_1(x)p_2(x),$$

其中 $1\leqslant\deg(p_1(x)),\deg(p_2(x))<\deg(p(x))$.

根据主理想的结构,不难得到$(p(x))\subset(p_1(x))\neq F[x]$,这与$(p(x))$是 $F[x]$中的极大理想相矛盾. 结论得证.

推论 3.7.1 设 $p(x)$是多项环 $F[x]$中的一个多项式,则商环 $F[x]/(p(x))$是域当且仅当 $p(x)$是一个不可约多项式.

证明 充分性. 设 $p(x)$是一个不可约多项式. 由定理 3.7.7 可知,$p(x)$生成的理想$(p(x))$是极大理想. 再由定理 3.7.2 可知,$F[x]$是含幺交换环. 最后根据定理 3.3.6 可知,$F[x]/(p(x))$是一个域.

必要性. 设商环 $F[x]/(p(x))$是域. 由定理 3.7.2 可知,$F[x]$是含幺交换环. 再由定理 3.3.6 可知,$(p(x))$是极大理想. 最后由定理 3.7.7 可得,$p(x)$是一个不可约多项式.

定理 3.7.8 设 F 是域,$p(x),f_1(x),f_2(x),\cdots,f_m(x)\in F[x]$,且 $p(x)$是不可约多项式. 如果 $p(x)\mid f_1(x)f_2(x)\cdots f_m(x)$,则 $p(x)$一定整除至少其中的一个因式.

证明 由推论 3.7.1 可知,$Q=F[x]/(p(x))$是域. 我们考察这个域的结构.

用$[f_j(x)]$表示 Q 中 $f_j(x)$，$j=1,2,\cdots,m$ 所在的等价类，由题设知在 Q 中

$$[f_1(x)]\cdot[f_2(x)]\cdots[f_m(x)]=[f_1(x)\cdot f_2(x)\cdots f_m(x)]=[0].$$

因为 Q 没有零因子，所以至少有一个$[f_j(x)]=[0]$，即 $f_j(x)\in(p(x))$. 所以 $p(x)\mid f_j(x)$.

由素理想的定义和不可约多项式的这个性质，不难得到不可约多项式生成的理想也是素理想. 也就是说，$F[x]$中的极大理想也是素理想.

另外这个定理的结论，使我们也把不可约多项式称为素多项式，它实际上是环 $F[x]$ 中的一个素元.

因为 $F[x]$是主理想环，而主理想环一定是唯一分解环，于是有：

定理 3.7.9 （唯一分解）设 $f(x)$是域 F 上的一个正次数多项式. 那么 $f(x)$一定可以写成

$$f(x)=ap_1(x)^{k_1}p_2(x)^{k_2}\cdots p_l(x)^{k_l},$$

其中 $a\in F$，$p_i(x)(i=1,2\cdots,l)$是不同的不可约多项式，$k_i\geqslant 1$，$i=1,2\cdots,l$，而且在忽略次序的情况下，这种分解是唯一的.

3.8 环和域在循环码中的应用

纠错编码是一种信道编码，在通信系统中，用于提高信号传输的可靠性. 下面我们使用环或域上的多项式来构造一种纠错码 ——循环码.

循环码是一类重要的线性码. 它具有严谨的代数结构，其性能易于分析，编码译码电路简单易于实现，所以应用很广泛.

我们先从线性码谈起. 为了提高信号传输的准确性，在信息编码时，需要加入些冗余信息，用来检错和纠错. 一个(n,k)线性分组码 C 是称为码字 c 的 n 维向量的集合. n 是码长，k 是信息位长. 一个向量的汉明重量是向量中非零分量的个数，零向量称为零码字. 在分组码 C 中所有非零码字的最小汉明重量称为分组码 C 的最小码距 d. 二元线性码是码字为 F_2 上的向量构成的集合. 如果二元线性码的最小码距为 d，则它能够纠正任意小于等于$\lfloor d-1/2\rfloor$个差错.

下面我们以一个例子给出构造线性(分组)码的一种方法.

例 3.8.1 一个(5,3)线性分组码的生成矩阵为

$$G=\begin{pmatrix}1&0&0&0&1\\0&1&0&1&1\\0&0&1&1&1\end{pmatrix}.$$

设 $m=(m_1,m_2,m_3)$ 为消息，$mG=c$ 为 m 的码字. 具体如下：消息集合 $M=\{(000)$, (001), (010), (011), (100), (101), (110), $(111)\}$，对应的编码为 $C=\{(00000)$, (11011), (01011), (10001), (10110), (01100), (11101), $(00111)\}$.

用生成矩阵构造的线性码关于向量的加法构成一个群，所以这种线性码也称为群码. 同样，一个$[n,k]$二元线性码也是 F_2^n(二元 n 维向量构成的向量空间)的 k 维子空间.

类似于例 3.8.1，我们给出一个(7,4)分组码，16 个码字分别为(0100011), (1000110), (0001101), (0011010), (0110100), (1101000), (1010001), (1100101), (1001011), (0010111), (0101110), (1011100), (0111001), (1110010), (1111111), (0000000). 由这些码字可以看出每个码字的右(左)循环移位得到的向量仍然是码字，具有这种性质的分组码称为循环码. 具体定义如下：

定义 3.8.1 设 C 为(n,k)线性码，若对于任意一个码字 $c=(a_{n-1},a_{n-2},\cdots,a_0)$，都有 $c'=(a_{n-2},\cdots,a_0,a_{n-1})$也是一个码字，则称 C 为循环码.

我们给出一种用多项式的方法构造循环码的方法.

设 F_q(q 为素数或素数幂)是 q 元域，$F_q[x]$表示 F_q 上的多项式环. $F(x)$为 F_q 上的一个 n 次多项式，$(F(x))$是 $F_q[x]$的一个理想，$F_q[x]/(F(x))$是商环，当 $F(x)$是 F_q 上的不可约多项式时，$(F(x))$是极大理想，从而 $F_q[x]/(F(x))$是域. 而 $F_q[x]/(F(x))$的元素为

$$\begin{aligned}F_q[x]/(F(x))&=\{[a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_0]\mid a_i\in F_q,1\leqslant i\leqslant n-1\}\\&\triangleq\{a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_0\mid a_i\in F_q,1\leqslant i\leqslant n-1\}.\end{aligned}$$

设 C 是一个 n 长码字集合，$c=(a_{n-1},a_{n-2},\cdots,a_0)$，$a_i\in F_p$ 是一个码字，令

$$f(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0\in F_q[x].$$

这样我们就在码字集合 C 与 $F_q[x]/(F(x))$建立了一一对应关系. 码字 c 对应的多项式称为码多项式.

定理 3.8.1 $F_q[x]/(x^n-1)$的一个子环 I 的原象 C 是循环码的充分必要条件是 I 是理想.

证明 必要性. 设子环 I 的原象集 C 是循环码，对于任意 I 中的多项式

$$f(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0,$$

以及 $F_q[x]/(x^n-1)$ 中任意多项式

$$g(x)=b_{n-1}x^{n-1}+b_{n-2}x^{n-2}+\cdots+b_1x+b_0.$$

我们只需证明 $f(x)g(x)\in I$ 即可.

设 $f(x)$ 的原象为 $c_1=(a_{n-1},a_{n-2},\cdots,a_0)\in C$,则

$$xf(x)=a_{n-1}x^n+a_{n-2}x^{n-1}+\cdots+a_1x^2+a_0x\equiv a_{n-2}x^{n-1}+\cdots+a_1x^2+a_0x+a_{n-1}(\mathrm{mod}(x^n-1))$$

$$x^2f(x)=a_{n-2}x^n+a_{n-1}x^{n-1}+\cdots+a_0x^2+a_{n-1}x\equiv a_{n-3}x^{n-1}+\cdots+a_{n-1}x+a_{n-2}(\mathrm{mod}(x^n-1))$$

$$\vdots$$

$$x^{n-1}f(x)=a_1x^n+a_0x^{n-1}+\cdots+a_2x\equiv a_0x^{n-1}+a_{n-1}x^{n-2}+\cdots+a_2x+a_1(\mathrm{mod}(x^n-1))$$

由于 C 是循环码,所以 $f(x),xf(x),\cdots,x^{n-1}f(x)$ 的原象均为码字,从而

$$f(x),xf(x),\cdots,x^{n-1}f(x)\in I.$$

$f(x)g(x)=b_{n-1}x^{n-1}f(x)+b_{n-2}x^{n-2}f(x)+\cdots+b_0f(x)$ 的原象为

$$b_{n-1}(a_{n-1},a_{n-2},\cdots,a_0)+b_{n-2}(a_{n-1},a_{n-2},\cdots,a_0)+\cdots+b_0(a_{n-1},a_{n-2},\cdots,a_0)\triangleq b.$$

由循环码的特性知道,$b\in C$,所以 $f(x)g(x)$ 是 b 的象,从而 $f(x)g(x)\in I$.

充分性. 因为 I 是理想,所以 I 的原象集 C 显然是线性码.

任取码字 $c_1=(a_{n-1},a_{n-2},\cdots,a_0)\in C$,其象为

$$f(x)=a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\cdots+a_1x+a_0\in I.$$

因为 I 是理想,所以 $xf(x)=a_{n-2}x^{n-1}+a_{n-3}x^{n-2}+\cdots+a_0x+a_1\in I$,$xf(x)$ 的原象为 $c_2=(a_{n-2},a_{n-3},\cdots,a_0,a_{n-1})$,从而 $c_2\in C$,这说明 C 是循环码.

从定理 3.8.1 中我们可以得到结论:一个循环码是商环 $F_q[x]/(x^n-1)$ 的一个理想,反之,此商环的一个理想必是循环码.

$F_q[x]/(x^n-1)$ 是主理想环,所以它的任意理想都是主理想,主理想的生成多项式称为码的生成多项式. 从而码多项式都是生成多项式的倍式.

这样,构造循环码的问题就转化为构造理想的生成多项式的问题. $F_q[x]/(x^n-1)$ 上的一个 $n-k$ 次多项式生成的主理想对应 F_q 上的一个 (n,k) 循环码. 事实上,设 $g(x)\in F[x]/(x^n-1)$ 是一个 r 次多项式,则

$$(g(x))=\{(m_{n-1-r}x^{n-1-r}+m_{n-2-r}x^{n-2-r}+\cdots+m_1x+m_0)g(x)\mid m_i\in F_q,0\leqslant m\leqslant n-1-r\}.$$

由此可见,由 $g(x)$ 生成的主理想中有 q^{n-r} 个元素,而 (n,k) 循环码共有 q^k 个码字,只需要求 $n-r=k$,即当 $r=n-k$ 时,由 $g(x)$ 生成的主理想对应一个 (n,k) 循环码.

由这些结论可以得到：

(1) 构造一个(n,k)循环码，就是找一个能除尽 x^n-1 的 $n-k$ 次多项式 $g(x)$，在 $F_2[x]/(x^n-1)$中，构造由 $g(x)$生成主理想.

(2) 主理想中的每个多项式就是一个码多项式，码多项式的原象就是码字.所有这些码字集合就是(n,k)循环码.

例 3.8.2　在 F_2 上构造一个(7,4)循环码.

解　首先 $x^7-1=(x+1)(x^3+x+1)(x^3+x^2+1)$，选 $g(x)=x^3+x^2+1$，则

$$xg(x)=x^4+x^3+x,$$

$$x^2g(x)=x^5+x^4+x^2,$$

$$x^3g(x)=x^6+x^5+x^3.$$

与它们对应的码字为(0001101)，(0011010)，(0110100)，(1101000).把它们作为生成矩阵的行，就得到了(7,4)循环码的生成矩阵.

$$\boldsymbol{G}=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\0&0&1&1&0&1&0\\0&0&0&1&1&0&1\end{bmatrix}$$

则 $\boldsymbol{C}=c\boldsymbol{G}(c\in F_2^7)$就是(7,4)循环码.

习　　题

1. 证明在 $Z\times Z$ 中定义加法和乘法如下：$(a,b)+(c,d)=(a+c,b+d)$，$(a,b)(c,d)=(ac,bd)$.其中(a,b)，(c,d)为 $Z\times Z$ 中的任意元素.求证：$Z\times Z$ 是一个有零因子的含幺交换环.

2. 设 R 是无零因子环，且只有有限个元素，证明 R 是除环.

3. 若环 R 的非零元素 e，满足 $e^2=e$，则称 x 为幂等元，证明若无零因子环 R 有幂等元 e，则 R 为含幺环，e 为 R 的幺元.

4. 若环 R 对于加法做成一个循环群，证明 R 是交换环.

5. 证明：若 R 是一个除环，则 R 中无零因子.

6. 证明：有限的整环一定是域.

7. 设 F 是一个有 4 个元素的域，证明：

(1) F 的特征是 2；

(2) F 中非零元和非幺元都满足 $x^2=x+1$.

8. 设$[a]$是模 n 的一个剩余类，证明：若$(a,n)=1$，则所有$[a]$中的数都与 n 互素.

9. 证明：所有与 n 互素的模 n 的剩余类对于剩余类的乘法做成一个群.

10. 证明：若$(a,n)=1$，则 $a^{\varphi(n)}\equiv 1(\bmod n)$（$\varphi(n)$表示与 n 互素且不超过 n 的正整数的个数）.

11. 求证：交换环 R 中全部幂零元素（即存在自然数 n，使 $a^n=0$ 的元素 $a,a\in R$）组成的集合 N 是环 R 的理想.

12. 找出模 6 剩余类环的所有理想.

13. 设 $I_1,I_2,\cdots,I_n\cdots$均是环 R 中的理想，并且 $I_1\subseteq I_2\subseteq\cdots\subseteq I_n\cdots$，求证：集合 $\bigcup_{j=1}^{\infty} I_j$ 也是环 R 的理想.

14. 求证 $T=\left\{\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| a,b,c\in Z\right\}$是全体二阶矩阵环 $M_2(Z)$的子环，并找出 T 的所有理想.

15. 设 R 是全体复数 $a+b\mathrm{i}(a,b\in Z)$按复数的加法和乘法做成的环，$R/(1+\mathrm{i})$中有多少个元素？$R/(1+\mathrm{i})$是域吗？

16. 设 R 是全体偶数做成的环，证明：(4)是 R 的极大理想，但 $R/(4)$不是域.

17. 设 f 是从环 R 到环 $\overline{R}$ 的一个同态满射，证明：f 是同构映射当且仅当 $\mathrm{Ker}(f)$是 R 的零理想.

18. 求证：含幺交换有限环的素理想一定是极大理想.

19. 写出模 12 的剩余类环 Z_{12}的全部理想，哪些是素理想，哪些是极大理想？

20. 令 $Z[\mathrm{i}]=\{m+n\mathrm{i}\mid m,n\in Z\}$，证明 $Z[\mathrm{i}]$是一个整环，并确定 $Z[\mathrm{i}]$的商域.

21. 令 $Z[\sqrt{2}]=\{m+n\sqrt{2}\mid m,n\in Z\}$，证明 $Z[\sqrt{2}]$是一个整环，并确定其商域.

22. 令 $R=Z(\sqrt{5})=\{a+b\sqrt{-5}\mid a,b\in Z\}$，$R$ 是唯一析因环吗？3 是 R 中的不可约元素吗？3 是素元吗？

23. 设 R 和 $\widetilde{R}$ 都是整环，R 是唯一析因环，又存在从 R 到 $\widetilde{R}$ 的满同态映射 φ，试问 $\widetilde{R}$ 是唯一析因环吗？

24. 证明 Gauss 整数环 $Z[\mathrm{i}]=\{a+b\mathrm{i}\mid a,b\in Z\}$是欧氏环.

25. 证明域一定是欧氏环.

26. 设 R 是整环, $R[x]$ 是 R 上的一元多项式环, $f(x), g(x) \in R[x]$. 证明: $\deg(fg) = \deg(f) + \deg(g)$. 试问对一般的交换幺环, 上式是否成立?

27. 设 Q 是有理数域, $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}\mathrm{i}$, 证明 w 在 Q 上是代数的, 且 $Q[w] \cong Q[x]/(x^2+x+1)$.

28. 设 R 是整环, 求证 R 上的一元多项式环 $R[x]$ 也是整环.

29. 设 $R[x]$ 是含幺元的交换环 R 上的一元多项式环. 证明: $0 \neq f(x)$ 是 $R[x]$ 的零因子的充分必要条件是存在 $0 \neq c \in R$, 使 $cf(x) = 0$.

第4章　扩　　域

通过理想研究环,是研究环的基本方法,但是,域只有平凡理想,因此这种方法不适合对域的研究.研究域的最基本的方法是对域进行扩张,这种域的扩张起源于数域的扩张.

本章主要讨论单扩域、代数扩域、分裂域和有限域等.我们虽然只研究了它们的基本性质,但通过这些简单性质可以让我们理解研究域的最基本的方法.

4.1　域的单扩张

4.1.1　素域与扩域的概念

定义 4.1.1　如果域 F 是域 E 的子域,则称域 F 为 E 的一个扩域.

例如,复数域是实数域的扩域,而复数域和实数域又都是有理数域的扩域.有理数域是最小的数域,它不含任何真子域.

定义 4.1.2　如果一个域不含真子域,就称它是一个素域.

可见,有理数域是一个素域.另外,当 p 为素数时, Z_p 也是素域.实际上,在同构意义下,它们是所有的素域.

定理 4.1.1　若域 E 的特征为零,则 E 包含一个与有理数域同构的素域;若 E 的特征为素数 p,则 E 包含一个与 Z_p 同构的素域.

证明　考虑 E 中的子集

$$R=\{ne \mid e\text{ 是 }E\text{ 的单位元},n\text{ 为整数}\}.$$

则 R 是 E 的子环.

作整数环到 R 的映射 $f:Z\to R$ 为

$$f(n)=ne,$$

则 f 是从 Z 到 R 的满同态映射. 也就是整数环 Z 与 R 同态.

分情形讨论如下：

(1) 当 E 特征为零时，$\ker(f)=\{0\}$，f 为同构映射，即

$$Z\cong R.$$

由定理 3.4.5 可知，Z 的商域与 R 的商域同构. Z 的商域是有理数域，R 的商域是包含 R 的最小的域，也就是 E 的一个素域. 因此 R 的商域，即 E 的一个素域与有理数域同构.

E 包含 R 的商域. 因此 E 包含了一个与有理数域同构的子域，这个子域显然是素域.

(2) 当 E 的特征是素数 p 时，由环同态基本定理，有

$$Z/\ker(f)\cong R.$$

而

$$\ker(f)=(p),$$

其中，(p)表示由 p 生成的理想. 因此

$$Z/(p)\cong Z_p\cong R.$$

而 Z_p 明显是一个素域. 因此 R 也是一个素域. 也就是说若 E 的特征为素数 p，则 E 包含了一个与 Z_p 同构的素域.

由这个定理我们可以直接得到下面两个推论.

推论 4.1.1 设 K 是一个素域，当它的特征为零时，K 与有理数域同构. 当它的特征是素数 p 时，K 与 Z_p 同构.

另外由定理的证明过程，可以看出，若记域 E 的单位元为 e，则

$$K=\left\{\frac{me}{ne}\mid m,n\in Z,ne\neq 0\right\}$$

是 E 的一个素子域. 在同构意义下是 E 的唯一素子域.

推论 4.1.2 每个域都包含一个素域且仅只包含一个素域.

4.1.2 扩域的结构

设 E 是域 F 的一个扩域. 从 E 中取出一个子集 S，用 $F(S)$表示 E 的包含 F 和 S 的最小子域，称之为添加集合 S 于 F 所得的扩域. 易见 $F(S)$是 E 中包含 F 和 S 的所有子域的交集. 事实上，可以证明

$$F(S)=\left\{\frac{f(\alpha_1,\alpha_2,...\alpha_n)}{g(\alpha_1,\alpha_2,...\alpha_n)}\middle|\alpha_i\in S,1\leqslant i\leqslant n,n\in N\right\}.$$

其中 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是 S 中任意有限个元素，$f(\alpha_1,\alpha_2,\cdots,\alpha_n)$，$g(\alpha_1,\alpha_2,\cdots,\alpha_n)$是系数取自 F 的关于 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 的任意多项式，当然 $g(\alpha_1,\alpha_2,\cdots,\alpha_n)\neq 0$.

适当选取集合 S，可以使 $E=F(S)$，因此 E 是一切添加 S 于 F 所得子域的交集. 接下来，我们讨论 S 为有限集的情形. 设 $S=\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$，记 $F(S)$为 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$.

定理 4.1.2 令 E 是域 F 的一个扩域，S_1,S_2 是 E 的两个子集. 那么

$$F(S_1)(S_2)=F(S_1\cup S_2)=F(S_2)(S_1).$$

证明 $F(S_1)(S_2)$是包含 $F(S_1)$与 S_2 的域，当然也是包含 F,S_1,S_2 的域，从而是包含 F 与 $S_1\cup S_2$ 的域. 但是 $F(S_1\cup S_2)$是包含 F 与 $S_1\cup S_2$ 的最小的域，故

$$F(S_1\cup S_2)\subseteq F(S_1)(S_2).$$

另一方面，$F(S_1\cup S_2)$包含 F 与 $S_1\cup S_2$，从而也包含 F,S_1,S_2，当然也包含 $F(S_1)$与 S_2. 但 $F(S_1)(S_2)$是包含 $F(S_1)$与 S_2 的最小的域，所以

$$F(S_1)(S_2)\subseteq F(S_1\cup S_2).$$

因此

$$F(S_1)(S_2)=F(S_1\cup S_2).$$

类似可以证明

$$F(S_2)(S_1)=F(S_1\cup S_2).$$

根据这个定理，我们有

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1)(\alpha_2)\cdots(\alpha_n).$$

这样对扩域 $F(\alpha_1,\alpha_2,\cdots,\alpha_n)$的研究，可以归结为对向 F 添加一个元素而得到的扩域的研究，即是下面讨论的单代数扩域.

4.1.3 域的单扩域(张)

定义 4.1.3 设 E 是 F 的一个扩域，$\alpha\in E$. 添加元素 α 于域 F 的扩域 $F(\alpha)$称为 F 的一个单扩域，或单扩张.

定义 4.1.4 设 E 是 F 的一个扩域，$\alpha\in E$. 如果存在 F 中不全为零的元素 $a_0,a_1,\cdots,a_n$，使

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_n\alpha^n=0,$$

则称 α 为 F 上的代数元. 否则称 α 为 F 上的一个超越元.

当 α 是 F 上的代数元(超越元)时，$F(\alpha)$称为 F 的一个单代数扩张(单超越扩张).

例如，$\sqrt{2}$，i 都是有理数域上的一个代数元，圆周率 π 是有理数域上的一个超越元. 但圆周率 π 是实数域上的一个代数元.

下面讨论单扩域的结构.

定理 4.1.3 若 α 是 F 上的一个超越元,则 $F(\alpha)\cong F[x]$的商域;若 α 为 F 上的一个代数元,则 $F(\alpha)\cong F[x]/(p(x))$,其中 $p(x)\in F[x]$是一个唯一确定的首项系数为 1 的不可约多项式,且 $p(\alpha)=0$.

证明 考虑映射 $f:F[x]\to F[\alpha]$,

$$f\left(\sum_{i=0}^{n}a_ix^i\right)=\sum_{i=0}^{n}a_i\alpha^i,$$

则 f 是一个满同态映射. 分情形如下:

(1) 当 α 是 F 上的超越元时,$\ker(f)=\{0\}$,f 是同构映射. 因此 $F[x]$的商域与 $F[\alpha]$的商域同构. 而 $F(\alpha)$的商域就是 $F(\alpha)$. 因此 $F(\alpha)\cong F[x]$的商域.

(2) 当 α 是 F 上的代数元时,由环同态基本定理,

$$F(\alpha)\cong F[x]/\ker(f).$$

由定理 3.7.4 可知,$F[x]$是一个主理想环,所以 $\ker(f)=(p(x))$,$p(x)\in F[x]$是一个不可约多项式,在首项系数为 1 的前提下,它是唯一确定的. 再者,$F[x]/\ker(f)$中的零元$(p(x))$,它的象 $p(\alpha)$是 $F(\alpha)$上的零元,所以有 $p(\alpha)=0$.

最后由推论 3.7.1 可知,$F[x]/(p(x))$是一个域,因此 $F(\alpha)\cong F[x]/(p(x))$.

4.1.4 单扩域的存在性与唯一性

前面我们给出了单扩域的结构,那么给定域 F 以后,是否有 F 的单扩域存在呢? 单超越扩域的存在性比较容易看出. 事实上,F 上的未定元 x 就是 F 上的一个超越元,$F[x]$的商域就是一个单超越扩域. 由定理 4.1.3 可知,F 的所有单超越扩域都是同构的.

定义 4.1.5 $F[x]$中满足 $p(\alpha)=0$ 的次数最低的首项系数为 1 的多项式

$$p(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+x^n$$

称为 α 的极小多项式. n 称为 α 在 F 上的次数.

关于单代数扩域的存在唯一性,我们有下面的结论.

定理 4.1.4 对于域 F 及 $F[x]$中的给定不可约多项式

$$p(x)=a_0+a_1x+a_2x^2+\cdots+a_{n-1}x^{n-1}+x^n,$$

总存在 F 的单代数扩域 $F(\alpha)$,使 α 在 F 上的极小多项式为 $p(x)$.

证明 因为 $p(x)$为不可约多项式,由定理 3.7.7 可知,$(p(x))$是一个极大理想. 令

$$\overline{K}=F[x]/(p(x)),$$

由定理 3.3.6 可知，$\overline{K}$是一个域.

考虑映射 $\phi: F[x] \to \overline{K}$,

$$f(x) \to \overline{f(x)} = [f(x)].$$

这是一个同态满射. 在该映射下 F 与它的象$\overline{F}$同构.

由定理 3.4.1 可知，存在与$\overline{K}$同构的域 K，使 $F \subset K$. 令$\overline{x}$在 K 中的原象为 α，则

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} + \alpha^n = 0,$$

从而 α 为域 F 上的代数元，α 在 F 上极小多项式为 $p(x)$. 又

$$F[\alpha] = F(\alpha) \cong \overline{K} = F[x]/(p(x)),$$

因此 $K = F(\alpha)$.

定理 4.1.4 告诉我们，给定 F 及 $F[x]$中首一不可约多项式 $p(x)$，一定存在 F 的单代数扩域 $F(\alpha)$，使得 α 在 F 上的极小多项式为 $p(x)$. 再由定理 4.1.3 可知，若另有 F 的单代数扩域 $F(\beta)$，β 的极小多项式也为 $p(x)$，则 $F(\alpha) \cong F(\beta) \cong F[x]/(p(x))$. 因此从同构意义来讲，以 $p(x)$为极小多项式的单扩域是存在的，且是唯一的.

4.2 代数扩域(张)

由 4.1 节可以看到，单代数扩域和单超越扩域的结构是不同的. 但一般来说，对于域 F 的扩域 E，域 E 的元素有些可能是 F 的代数元，有些可能是 F 的超越元. 这一节我们讨论扩域中的每个元素都是某一子域上的代数元的域结构.

4.2.1 有限扩域

定义 4.2.1 若 F 的扩域 E 中的每一个元素都是 F 上的代数元，则称 E 为 F 的一个代数扩域，或代数扩张.

假定 E 是 F 的扩域，我们将 F 视为数域，F 与 E 中元素的乘法可以视为数乘，容易验证对于 E 的加法及 E 的乘法来说，E 就作成了 F 上的一个向量空间. E 或者是 F 上的有限维向量空间，或者是无限维空间.

定义 4.2.2 设 E 是 F 的扩域，若 E 作为 F 上的向量空间是 n 维的，则称 n 为扩域 E 在 F 上的次数，记为$(E:F)$，此时 E 称为 F 的有限扩域，否则 E 称为 F 的无限扩域.

定理 4.2.1 设 K 是 F 的有限扩域，E 是 K 的有限扩域，则 E 也是 F 的有限扩域，

且

$$(E:F)=(E:K)(K:F).$$

证明　设$(E:K)=n,(K:F)=m$.

设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 为 E 在 K 上的一组基,$\beta_1,\beta_2,\cdots,\beta_m$ 为 K 在 F 上的一组基. 下面证明 $\alpha_i\beta_j,1\leqslant i\leqslant n,1\leqslant j\leqslant m$, 这 mn 个元素是 E 在 F 上的基.

任取 $\theta\in E$,因为 E 是 K 上向量空间,所以存在 $y_1,y_2,\cdots,y_n\in K$,使得

$$\theta=\sum_{j=1}^{n}y_j\alpha_j.$$

又 K 是 F 上的向量空间,所以存在 $x_{1j},x_{2j},\cdots,x_{nj}\in F$,使

$$y_j=\sum_{i=1}^{m}x_{ij}\beta_i,j=1,2,\cdots,m,$$

从而有

$$\theta=\sum_{j=1}^{n}y_j\alpha_j=\sum_{j=1}^{n}(\sum_{i=1}^{m}x_{ij}\beta_i)\alpha_j.$$

这表明 E 中所有元素都是 $\alpha_i\beta_j,1\leqslant i\leqslant n,1\leqslant j\leqslant m$ 的组合.

接下来说明 $\alpha_i\beta_j,1\leqslant i\leqslant n,1\leqslant j\leqslant m$ 在 F 上线性无关.

设

$$\sum_{j=1}^{n}\sum_{i=1}^{m}k_{ij}\beta_i\alpha_j=\sum_{j=1}^{n}(\sum_{i=1}^{m}k_{ij}\beta_i)\alpha_j=0.$$

因为 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 线性无关,所以有

$$\sum_{i=1}^{m}k_{ij}\beta_i=0,\quad j=1,2,\cdots,n.$$

又 $\beta_1,\beta_2,\cdots,\beta_m$ 线性无关,故

$$k_{ij}=0,i=1,2,\cdots,n,\quad j=1,2,\cdots,m.$$

也就是,$\alpha_i\beta_j,1\leqslant i\leqslant n,1\leqslant j\leqslant m$ 是 E 在 F 上的基. 显然还有$(E:F)=(E:K)(K:F)$.

这个结论可推广到有限个子域的情形. 即若 $F\subset K_1\subset K_2\subset\cdots\subset K_s\subset E$,后面是前面的有限扩域,则 E 也是 F 的有限扩域,且有

$$(E:F)=(E:K_s)(K_1:F)\prod_{2\leqslant i<j\leqslant s-1}(K_i:K_j).$$

4.2.2　代数扩域与有限扩域

定理 4.2.2　若 $E=F(\alpha)$是 F 的单代数扩张,则 E 是 F 的一个代数扩张.

证明 设β是E中的任意元素，下面证明它是F上的代数元.

设α在F上的极小多项式的次数为n，则$E=F(\alpha)=F[\alpha]$，E中每一个元素都可以唯一地表示为

$$a_0+a_1\alpha+a_2\alpha^2+\cdots+a_{n-1}\alpha^{n-1}$$

的形式，其中$a_0,a_1,\cdots,a_{n-1}\in F$.

这说明$1,\alpha,\alpha^2,\cdots,\alpha^{n-1}$是$E$在$F$上的一组基. 因此$(E:F)=n$.

n维向量空间中$n+1$个元素一定是线性相关的，因此

$$1,\beta,\beta^2,\cdots,\beta^{n-1},\beta^n$$

是线性相关的，于是存在不全为零的元素$b_0,b_1,\cdots,b_n\in F$，使

$$b_0+b_1\beta+\cdots+b_n\beta^n=0,$$

所以β是F上的代数元.

由定理4.2.2的证明，可得：

推论4.2.1 F的单代数扩域$F(\alpha)$是F的一个n次扩张，其中n是α在F上的极小多项式的次数.

推论4.2.2 F的有限扩域一定是F的代数扩域.

定理4.2.3 设$E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，其中$\alpha_i$是域$F$上的代数元，$1\leqslant i\leqslant n$. 则$E$是$F$的有限扩域，因而是代数扩域.

证明 用数学归纳法. 当$n=1$，结论正确.

假设$E=F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$是有限扩张，那么

$$F(\alpha_1,\alpha_2,\cdots,\alpha_n)=F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})(\alpha_n).$$

因为α_n是F上的代数元，因而也是$F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$上的代数元. 所以$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})$的单代数扩域，由定理是4.2.2可知，$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是有限扩域. 于是

$$F\subset F(\alpha_1,\alpha_2,\cdots,\alpha_{n-1})\subset F(\alpha_1,\alpha_2,\cdots,\alpha_n),$$

再由定理4.2.1，可知$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$F$上的有限扩域.

通过上面的讨论，我们得知，当$\alpha_1,\alpha_2,\cdots,\alpha_n$是$F$的代数元时，$F(\alpha_1,\alpha_2,\cdots,\alpha_n)$是$F$的有限次扩域. 反之，$F$的有限扩域就是添加有限个代数元于$F$而得到的扩域.

推论4.2.3 域F上的两个代数元的和，差，积，商(分母非零)仍是F上的代数元.

证明 设α,β是F上的任意两个代数元. 由定理4.2.3，$F(\alpha,\beta)$是F上的代数扩域. 而α,β的和，差，积，商都是$F(\alpha,\beta)$中元素，所以都是F上的代数元.

定理 4.2.4　设 E 是 F 的一个扩域，S 是 E 的一个非空集合，且 S 只含域 F 上的代数元，则 $F(S)$ 是 F 的代数扩域.

证明　任取 $\beta \in F(S)$，则存在 $\alpha_1, \alpha_2, \cdots, \alpha_n \in S$，使

$$\beta = \frac{f(\alpha_1, \alpha_2, \cdots, \alpha_n)}{g(\alpha_1, \alpha_2, \cdots, \alpha_n)}, \quad f, g \in F[x_1, x_2, \cdots, x_n].$$

显然 $\beta \in F(\alpha_1, \alpha_2, \cdots, \alpha_n)$. 由定理 4.2.3，$F(\alpha_1, \alpha_2, \cdots, \alpha_n)$ 是 F 的代数扩域，故 β 是 F 上的代数元. 从而 $F(S)$ 是 F 的代数扩域.

可以看出，S 可以是有限集，也可以是无限集. S 如果是有限集合，则定理 4.2.4 与定理 4.2.3 等价. 当 S 是无限集时，注意 $F(S)$ 虽然是代数扩域，但不一定是有限次扩张.

例如，令

$$S = \{\sqrt[i]{2} \mid i = 2, 3, \cdots\},$$

由于 S 中的每个元素都是有理数域上的代数元. 故由定理 4.2.3 可知，$Q(S)$ 是有理数域 Q 的代数扩域. 但它不是 Q 上的有限扩域.

因为，如果 $(Q(S):Q) = n$，则由于 $\sqrt[n+1]{2}$ 在 Q 上的最小多项式是

$$x^{n+1} - 2.$$

故

$$(Q(S):Q) = n + 1.$$

这与 $(Q(S):Q) = n$ 相矛盾. 因此 $Q(S)$ 是 Q 上的无限扩域.

这就是说，代数扩域不一定是有限扩域.

4.3　分 裂 域

我们知道，数域 P 上的 n 次多项式 $f(x)$ 在 P 上不一定有解，如果有解，也不一定有 n 个. 由代数基本定理，在复数域上，$f(x)$ 一定有 n 个解，当然也能分解成一次因式的乘积.

类似地，域 F 上的多项式 $f(x)$ 在 F 中不一定有解. 本节将要说明的是：可以将 F 扩张，使 $f(x)$ 在扩域中有解，且扩域包含这个多项式的所有解.

4.3.1　分裂域的概念

定义 4.3.1　设 E 是 F 的扩域，$f(x) \in F[x]$. 如果在 $E[x]$ 中 $f(x)$ 可以分解为一次

因式的乘积：

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

其中 $\alpha_1,\alpha_2,\cdots,\alpha_n\in E, a\in F$ 为首项系数. 并且在一个小于 E 的中间域 K 中，$f(x)$ 不能这样分解，则 E 称为 $f(x)$ 的一个分裂域或根域.

由定义可以看出，E 是包含 F 和 $f(x)$ 的所有解的最小域.

例 4.3.1 多项式 x^2-2 在有理数域上的一个分裂域是 $Q(\sqrt{2})$. 但它在实数域上的分裂域就是实数域本身.

定理 4.3.1 设 $f(x)$ 是域 F 上的多项式，令 E 是 $f(x)$ 在 F 上一个分裂域. 且

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

其中 $\alpha_1,\alpha_2,\cdots,\alpha_n\in E, a\in F$，则

$$E=F(\alpha_1,\cdots,\alpha_n).$$

证明 因为 $F(\alpha_1,\cdots,\alpha_n)$ 是域，且有

$$F\subseteq F(\alpha_1,\cdots,\alpha_n)\subseteq E,$$

而 $f(x)$ 在 $F(\alpha_1,\cdots,\alpha_n)$ 中可以完全分解，E 又是 $f(x)$ 在 F 的分裂域，故 $E=F(\alpha_1,\cdots,\alpha_n)$.

这个定理告诉我们，$f(x)$ 在 F 上的分裂域就是添加 $f(x)$ 的全部根于 F 所得到的扩域，这也就是将 $f(x)$ 的分裂域称为根域的原因. 当然 $f(x)$ 的分裂域是 F 上的一个有限扩域，所以分裂域是 F 的一个代数扩域.

例 4.3.2 求多项式 $f(x)=x^3-1$ 在有理数域 Q 上和实数域上的分裂域.

解 因为

$$f(x)=(x-1)\left(x-\frac{-1+\sqrt{3}\mathrm{i}}{2}\right)\left(x-\frac{-1-\sqrt{3}\mathrm{i}}{2}\right),$$

由定理 4.3.1，$f(x)$ 在 Q 上的分裂域为

$$Q\left(1,\frac{-1+\sqrt{3}\mathrm{i}}{2},\frac{-1-\sqrt{3}\mathrm{i}}{2}\right)=Q(\sqrt{3}\mathrm{i}).$$

所以 $f(x)$ 在 Q 上的分裂域为 $Q(\sqrt{3}\mathrm{i})$，即由一切复数 $a+b\sqrt{3}\mathrm{i}(a,b\in Q)$ 构成的数域.

$f(x)$ 在实数域 R 上的分裂域为

$$R\left(1,\frac{-1+\sqrt{3}\mathrm{i}}{2},\frac{-1-\sqrt{3}\mathrm{i}}{2}\right)=R(\mathrm{i}),$$

所以 $f(x)$ 在 R 上的分裂域就是复数域.

4.3.2 分裂域的存在性

定理 4.3.2 设 $f(x)$是 F 上的 n 次多项式，$n\geqslant 1$，则 $f(x)$在 F 上的分裂域 E 一定存在.

证明 对多项式的次数 n 进行数学归纳.

当 $n=1$ 时，F 本身就是 $f(x)$的分裂域.

假设次数$<n$ 的多项式 $f(x)$在 F 上的分裂域存在.

当多项式 $f(x)$的次数为 $n(n>1)$时. 设 $p(x)$是 $f(x)$在 F 上的一个首项系数为 1 的不可约因式. 由定理 4.1.4 可知，存在域 $E_1=F(\alpha_1)$，其中 α_1 在 F 上的极小多项式是 $p(x)$. 故在 E_1 中 $p(\alpha_1)=0$，因此 $f(\alpha_1)=0$，即

$$x-\alpha_1 \mid f(x).$$

因此在 E_1 中

$$f(x)=(x-\alpha_1)f_1(x).$$

其中 $f_1(x)$是 E_1 上的次数$=n-1<n$ 的多项式.

由归纳假设，$f_1(x)$在 E_1 上存在分裂域

$$E_2=E_1(\alpha_2,\cdots,\alpha_n).$$

令

$$E=E_2(\alpha_1),$$

由定理 4.1.2 可知，

$$E=E_2(\alpha_1)=E_1(\alpha_2,\cdots,\alpha_n)(\alpha_1)=F(\alpha_1,\alpha_2,\cdots,\alpha_n),$$

并且 $f(x)$在 E 上有分解式

$$f(x)=a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n),$$

即 E 是 $f(x)$在 F 上的分裂域.

定理 4.3.3 令 E 是多项式 $f(x)$在 F 上的分裂域，而 β 是 E 上的一个任意元，则 β 在 F 上的极小多项式在 $E[x]$中能分解成一次多项式的乘积.

证明 设 $E=F(\alpha_1,\alpha_2,\cdots,\alpha_n)$，假设 β 在 F 上的极小多项式 $g(x)$不能在 $E[x]$中分解为一次因式的乘积.

设在 $E[x]$中

$$g(x)=(x-\beta)p(x)g_1(x),$$

其中 $p(x)$是 $E[x]$中首项系数为 1 的不可约多项式，次数 $\deg(p(x))=m>1$.

设 β' 为 $p(x)$ 的一个根，作单扩域

$$E(\beta')=F(\alpha_1,\alpha_2,\cdots,\alpha_n,\beta').$$

由于

$$g(\beta')=(\beta'-\beta)p(\beta')g_1(\beta')=0,$$

由定理 4.1.4 可知，即

$$F(\beta',\alpha_1,\alpha_2,\cdots,\alpha_n)\triangleq F(\beta,\alpha_1,\alpha_2,\cdots,\alpha_n),$$

而

$$F(\beta,\alpha_1,\alpha_2,\cdots,\alpha_n)=E(\beta)=E, F(\beta',\alpha_1,\alpha_2,\cdots,\alpha_n)=E(\beta'),$$

这与 $(E(\beta'):E)=\deg(p(x))=m>1$ 矛盾. 这说明 β 在 F 上的极小多项式在 $E[x]$ 中能分解成一次多项式的乘积.

4.4 有限域

这一节我们介绍有限域的一些基本性质. 有限域由于含有有限个元素，所以它的结构比较清晰，而且有着许多特殊的性质. 所以有限域在计算机科学，通信理论和组合理论等方面有很多应用.

4.4.1 有限域的构造

含有有限个元素的域，称为有限域.

设 F 是一个有限域. 它的特征必然是某个素数 p，由定理 4.1.1 可知，F 包含素域 Z_p. 设 F 对 Z_p 的扩张次数为 n，那么 F 可以视为 Z_p 上的 n 维向量空间，设 $\alpha_1,\alpha_2,\cdots,\alpha_n$ 是一组基，则

$$F=\{k_1\alpha_1+k_2\alpha_2+\cdots+k_n\alpha_n \mid k_i\in Z_p, 1\leqslant i\leqslant n\}.$$

显然，

$$|F|=p^n.$$

由上面的讨论我们得到：

定理 4.4.1 设 F 是一个有限域，它的特征为素数 p，若 $(F:Z_p)=n$，则 F 所含元素的个数是 p^n.

有限域也称伽罗华(Galois)域，记为 $GF(p^n)$ 或 F_{p^n}，其中素数 p 是它的特征，n 是它

在其素子域上的次数.

利用向量空间的方法可以表示 F 中的元素. 下面我们给出域元素的另一种表示方法,这种方法更直接具体.

$p(x)$是 $F[x]$上的一个 $n(n\geqslant 1)$次不可约多项式,则$(p(x))$是 $F[x]$的一个极大理想,所以 $F[x]/(p(x))$是一个域. 且

$$F[x]/(p(x))=\{[a_0+a_1x+\cdots+a_{n-1}x^{n-1}]\mid a_i\in F,0\leqslant i\leqslant n-1\}.$$

为简单起见,我们将[0]记为 0,非零的剩余类简记为其中次数最低的首一多项式形式,即

$$F[x]/(p(x))\triangleq\{a_0+a_1x+\cdots+a_{n-1}x^{n-1}\mid a_i\in F,0\leqslant i\leqslant n-1\}.$$

这样,容易看出,若 $F=Z_p$,即$|F|=p$(p 元域),则

$$|F[x]/(p(x))|=p^n.$$

特别地,当 $p(x)$是一次多项式时,$|F[x]/(p(x))|=p$,即$|F[x]/(p(x))|=|F|$.

实际上,$F[x]/(p(x))$为添加 $F[x]$中的不可约多项式 $p(x)$的根 x 到 F 上而得到的域(代数扩域).

特别地,$F=Z_p$,$Z_p[x]/(p(x))$是含 p^n 个元素的有限域,而 Z_p 为一个子域.

另外,我们知道,$p(x)$的分裂域也是含有 p^n 个元素的域,而具有相同元素的有限域是同构的. 所以实际上还可以通过构造 $n(n\geqslant 1)$次不可约多项式 $p(x)$的分裂域来得到含 p^n 个元素的有限域.

当然不管由哪种方法构造有限域,只要它们所含元素的个数是相同的,它们就都同构.

我们总结为下面结论.

定理 4.4.2　对任意素数 p 及正整数 n,都存在一个恰含 p^n 个元素的有限域. 在同构意义下是唯一的,即 F_{p^n}(也记为 $GF(p^n)$).

例 4.4.1　令 $p=2$,$Z_2[x]$中的多项式 $p(x)=x^2+x+1$,因为 $p(0)=1\neq 0$,$p(1)=1\neq 0$,所以 $p(x)$在 $Z_2[x]$中不可约. 故 $Z_2[x]/(x^2+x+1)$恰含有 $2^2=4$ 个元素的有限域. 事实上,

$$Z_2[x]/(x^2+x+1)=\{0,1,x,x+1\}.$$

它的运算表如下:

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	1	0
$x+1$	$x+1$	x	1	0

$\otimes$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

值得注意的是，任意非零元 α 适合 $\alpha^3=1$，且对于 $x\neq 1$，有 $x^2\neq 1, x+1\neq 1, (x+1)^2\neq 1$，因此，$Z_2[x]/(x^2+x+1)$ 中任意非零元可表示成其中某一个元的方幂. 如 $x, x^2=x+1, x^3=1$.

例 4.4.2 设 $p=3$，考察 $Z_3[x]$ 中的多项式 $p(x)=x^2+1$，在 Z_3 中 $p(0)=1\neq 0$，$p(1)=2\neq 0$，$p(2)=2^2+1=2\neq 0$，所以 $p(x)$ 在 Z_3 中没有根，又因为 $p(x)$ 的次数为 2. 所以它在 Z_3 上不可约，于是

$$Z_3[x]/(x^2+1)=\{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}.$$

在 $Z_3[x]/(x^2+1)$ 中，任意非零元素 α 适合 $\alpha^{3^2-1}=\alpha^8=1$，而对于

$$\alpha=x+1, x+2, 2x+1, 2x+2,$$

都有

$$\alpha\neq 1, \alpha^2\neq 1, \cdots, \alpha^7\neq 1$$

因此每个元均可表示成它们的幂次，例如

$$\begin{array}{ccccc} x+1 & (x+1)^2 & (x+1)^3 & \cdots & (x+1)^8 \\ \| & \| & \| & \cdots & \| \\ x+1, & 2x, & 2x+1, & \cdots, & 1. \end{array}$$

4.4.2 有限域的性质

定理 4.4.3 设 F 是含有 q(素数幂)个元素的有限域，则 $\forall a\in F$，有

$$a^q=a.$$

证明 首先当 $a=0$ 时，结论显然成立. F 中所有的非零元组成一个 $q-1$ 阶乘群，所以有 $a^{q-1}=1$. 当然 $a^q=a$ 对所有非零元也成立.

由这个结论可以启示我们，含有 p^n 个元素的有限域可以看成是 $x^{p^n}-x$ 的分裂域.

定理 4.4.4 如果 E 是含有 q(素数幂)个元素的有限域，F 是它的一个子域，则 E 是

多项式 x^q-x 的分裂域.

证明 因为 x^q-x 在 F 中至多有 q 个根,根据定理 4.4.3,E 中的 q 个元素都是这个多项式的根.所以 x^q-x 在 E 中是分裂的,而且不能在任何更小的域中分裂.

定理 4.4.5 (子域准则)设 F_q 是一个具有 $q=p^n$ 个元素的有限域,则 F_q 的每一个子域含有 p^m 个元素,且 $m|n$.反之,对 n 的任一正因子 m,也存在唯一的含有 p^m 个元素的 F_q 的子域.

证明 因为 F_q 的特征是 p,所以它的每个子域的特征也是 p.由定理 4.4.1 可知,F_q 的每个子域所含的元素是 p 的某个方幂.

假设 K 是含 p^m 个元素的 F_q 的一个子域,m 是某个正整数.设 F_q 是 K 上的 r 维向量空间,即 $(F_q:K)=r$,从而

$$p^n=|F_q|=|K|^r=(p^m)^r=p^{mr},$$

故 $m|n$.

反之,假设 $m|n$,则 $p^m-1|p^n-1$,所以 $x^{p^m-1}-1|x^{p^n-1}-1$,因此,

$$x^{p^m}-x|x^{p^n}-x.$$

从而 $x^{p^m}-x$ 的分裂域为 F_q 的子域,且此子域含有 p^m 个元素.

如果 F_q 有两个不同的含有 p^m 个元素的子域,那么这两个子域中元素都是 $x^{p^m}-x$ 的根,因此这两个子域一定相同.

例 4.4.3 求 $F_{2^{12}}$ 的所有子域.

解 $F_{2^{12}}$ 的子域完全由 12 的因子决定.12 有 6 个因子 1,2,3,4,6,12.它们所对应的子域分别是 $F_2,F_{2^2},F_{2^3},F_{2^4},F_{2^6},F_{2^{12}}$.

4.5 扩域在循环码中的应用

我们继续讨论循环码.由 3.8 节的讨论我们知道,循环码对应于由多项式生成的理想.这样就通过寻找合适的多项式,构造其生成的理想,从而达到构造循环码的目的.

这一节,我们利用多项式在扩域上的根,给出循环码的另一种构造方法.

设多项式

$$g(x)=x^r+a_{r-1}x^{r-1}+\cdots+a_1x+a_0,\quad a_i\in F_q,\quad 0\leqslant a_i\leqslant r-1.$$

其中 F_q 为 q 元域，则 $g(x)$ 一定可以在 F_q 的一个扩域(分裂域)上完全分解.

当 $g(x)$ 有重根时，对应的码的性质通常比较差. 为此，我们首先找出 $g(x)$ 无重根的情况.

因为 $g(x)\mid x^n-1$，所以 $g(x)$ 的根也是 x^n-1 的根，这就要求 x^n-1 也没有重根. 而 F_q 上的多项式 x^n-1 没有重根的充分必要条件是 $(n,q)=1$. 可见当 $q=2$ 时，n 为奇数.

下面讨论 $g(x)$ 无重根时，如何用 $g(x)$ 的根构造循环码.

设 $g(x)$ 在 F 的扩域 F_{q^m} 上有完全分解

$$g(x)=(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_r),\quad \alpha_i\neq\alpha_j, i,j=1,2\cdots,r,$$

其中 $\alpha_i\in F_{q^m}$.

可知 $g(x)$ 有根 $\alpha_1,\alpha_2,\cdots,\alpha_r$. 码多项式都是 $g(x)$ 的倍式，因此每一个码多项式 $c(x)$ 也必以 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 为根. 设

$$c(x)=c_{n-1}x^{n-1}+c_{n-2}x^{n-2}+\cdots+c_1x+c_0,$$

则

$$c(\alpha_i)=c_{n-1}\alpha_i^{n-1}+c_{n-2}\alpha_i^{n-2}+\cdots+c_1\alpha_i+c_0=0,\quad i=1,2,\cdots,r.$$

写成矩阵形式

$$\begin{pmatrix}\alpha_1^{n-1} & \alpha_1^{n-2} & \cdots & \alpha_1 & 1\\ \alpha_2^{n-1} & \alpha_2^{n-2} & \cdots & \alpha_2 & 1\\ \vdots & \vdots & \vdots & \vdots & \vdots\\ \alpha_r^{n-1} & \alpha_r^{n-2} & \cdots & \alpha_r & 1\end{pmatrix}\begin{pmatrix}c_{n-1}\\ c_{n-2}\\ \vdots\\ c_1\\ c_0\end{pmatrix}=\boldsymbol{HC}^{\mathrm{T}}=0. \tag{4.1}$$

这说明若码多项式以 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 为根，则它对应的码字在矩阵 $\boldsymbol{H}$ 所确定的零空间中(即码字满足式(4.1)).

若 α_i 的极小多项式为 $m_i(x), i=1,2,\cdots,r$，则只有 $g(x)$ 和 $c(x)$ 同时能被 $m_i(x), i=1,2,\cdots,r$ 整除时，它们才能以 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 为根. 由于 $g(x)$ 是码多项式中次数最低的首一多项式，所以

$$g(x)=LCM(m_1(x),m_2(x),\cdots,m_r(x)).$$

$g(x)\mid(x^n-1)$，因此 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 也是 x^n-1 的根. 所以每个 $\alpha_1,\alpha_2,\cdots,\alpha_r$ 的阶能被 n 整除，由此可知循环码的码长

$$n=LCM(e_1,e_2,\cdots,e_r),$$

其中 $e_1, e_2, \cdots, e_r$ 分别为 $\alpha_1, \alpha_2, \cdots, \alpha_r$ 的阶数.

由前面的学习我们知道 F_{q^m} 乘法群是循环群,设 α 为 F_{q^m} 乘法群的生成元. 设 $\alpha_i = \alpha^k$,α_i 的极小多项式为 $m_i(x)$,则 $\alpha^k, \alpha^{kq}, \alpha^{kq^2}, \cdots, \alpha^{k(q^{m-1})}$ 也是 $m_i(x)$ 的根.

例 4.5.1 求 F_{2^4} 上以 $\alpha, \alpha^2, \alpha^4$ 为根的循环码.

设 α 为 F_{2^4} 的本原元,则它的极小多项式就是本原多项式 $m_1(x) = x^4 + x + 1$,$\alpha, \alpha^2, \alpha^4, \alpha^8$ 是它的根. 因此以 $\alpha, \alpha^2, \alpha^4, \alpha^8$ 为根的循环码,其生成多项式是 $g(x) = x^4 + x + 1$,码长 n 就是 α 的阶数,等于 $2^4 - 1 = 15$,由 3.8 节就得到了一个(15,11)循环码.

习 题

1. 设 E 是域 F 的一个扩域,而 $\alpha \in F$. 证明:α 是 F 上的一个代数元. 并且 $F(\alpha) = F$.

2. 求复数 i 和 $\frac{2i+1}{i-1}$ 在有理数域上的极小多项式,$Q(i)$ 与 $Q\left(\frac{2i+1}{i-1}\right)$ 是否同构.

3. 设 θ 是 $x^4 + 1 \in Q[x]$ 的一个根,在 $Q(\theta)$ 中将 $x^4 + 1$ 分解为不可约因式之积.

4. 写出 $\alpha = 1 + \sqrt{2}i \in C$ 在 Q 上的不可约多项式.

5. (1) 证明 $Q(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2} + \sqrt{3})$;

(2) 求 $[Q(\sqrt{2}, \sqrt{3}) : Q]$,并求 $Q(\sqrt{2}, \sqrt{3})$ 在 Q 上的一组基.

6. 求 $f(x) = x^3 - x^2 - x - 2$ 在有理数域 Q 上的分裂域.

7. 证明:有理数域 Q 上多项式 $x^4 + 1$ 的分裂域是一个单扩域 $Q(\alpha)$,其中 α 是 $x^4 + 1$ 的一个根.

8. 设 $f(x) = x^3 - a$ 是有理数域 Q 上的不可约多项式,而 β 是 $f(x)$ 的一个根. 证明:$Q(\beta)$ 不是 $f(x)$ 在 Q 上的分裂域.

9. 设 p 是一个素数,E 是 $x^p - 1$ 在 Q 上的分裂域. 证明:$(E:Q) = p - 1$.

10. 设 F 是有限域,证明 F 的乘群是循环群.

11. 证明对正整数 k,$a \in F_q^*$ 是 F_q 中某个元素的 k 次方幂当且仅当 $a^{\frac{(q-1)}{d}} = 1$,其中 $d = (q-1, k)$.

12. $f(x)$ 为 F_q 上的一个 n 次不可约多项式. 证明:$f(x)$ 整除 $x^{q^{n-1}} - x$.

参考文献

[1] 冯克勤,李尚志,查建国. 近世代数引论[M]. 中国科技大学出版社,1988 年.

[2] 胡冠章,王殿军. 应用近世代数(第三版)[M]. 清华大学出版社,2006 年.

[3] 杨子胥. 近世代数(第二版)[M]. 高等教育出版社,2003 年.

[4] 张禾瑞. 近世代数基础(修订本)[M]. 高等教育出版社,1978 年.

[5] 林东岱. 代数学基础与有限域[M]. 高等教育出版社,2006 年.

[6] 万哲先. 代数导引[M]. 科学出版社,2004 年.

[7] Rudolf Lidl, Harald Niederreiter, P. M. Cohn. Finite Fields[M]. Addison-Wesley Publishing Company,1983.

[8] Garrett Birkhoff,Saunders Mac Lane. A Survey of Modern Algebra[M]. Post & Telecom Press.

[General Information]
书名=近世代数应用基础
作者=张劼，莫骄编著
页数=106
SS号=12974343
DX号=
出版日期=2012.01
出版社=北京邮电大学出版社